

# DATA TERMINAL EQUIPMENT AND DATA RECORDING DEVICE

Publication number: JP2002366442

Publication date: 2002-12-20

Inventor: HORI YOSHIHIRO

Applicant: SANYO ELECTRIC CO

Classification:

- international: G06F12/14; G06F21/24; G06K19/073; H04L9/08; H04M11/00; H04N5/765; H04N5/907; H04N5/91; H04N7/167; G06F12/14; G06F21/00; G06K19/073; H04L9/08; H04M11/00; H04N5/765; H04N5/907; H04N5/91; H04N7/167; (IPC1-7): H04N5/765; H04N5/907; H04N5/91; G06F12/14; G06K19/073; H04L9/08; H04M11/00; H04N7/167

- European:

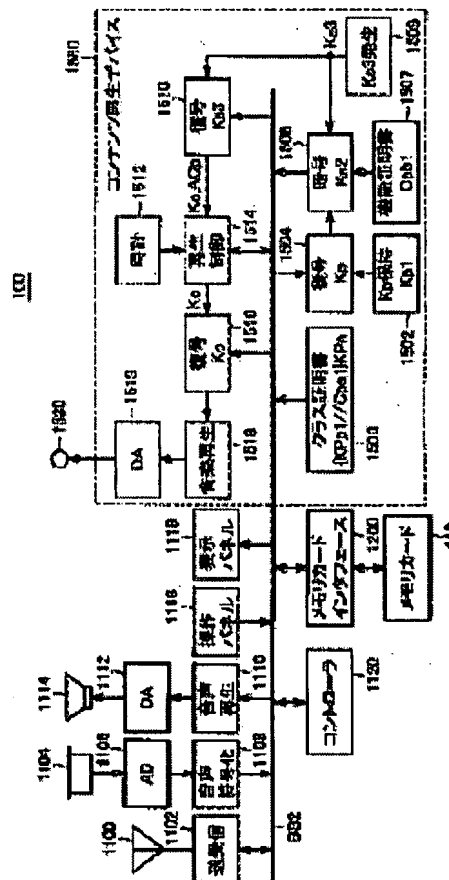
Application number: JP20010175036 20010611

Priority number(s): JP20010175036 20010611

Report a data error here

## Abstract of JP2002366442

**PROBLEM TO BE SOLVED:** To provide a data recording device and data terminal equipment corresponding to this data recording device capable of preventing the transfer of any license key corresponding to encrypted contents data under reproduction control which can not be controlled by a reproducing terminal or encrypted contents data which can not be reproduced by the reproducing terminal to the terminal equipment. **SOLUTION:** A portable telephone set 100 is provided with a function certificate holding part 1507 so that a function certificate Cbp1 can be transmitted to a memory card 110. Then, when a function certified by the function certificate is made correspond to a function limited by reproduction control information ACp, the portable telephone set 100 acquires the license key Kc for decoding encrypted contents data Dc)Kc and the reproduction control information ACp from the memory card 110. A reproduction control part 1514 judges the validity/invalidity of the reproduction of the encrypted contents data Dc)Kc based on time information from a clock 1512 and a reproduction period included in the reproduction control information ACp.



3

Cited reference 3: 2002-366442

[0044] FIG. 2 is a diagram showing data for communication to be used and characteristics of information and the like in the data distribution system shown in FIG. 1.

5 [0045] First, the data to be distributed from a distribution server 10 will be described. Symbol Dc is content data such as music data. The content data Dc is encrypted so that the data can be decrypted with a license key Kc. Encrypted content data {Dc}Kc encrypted so that the data can be decrypted with the license key Kc is distributed  
10 in this form from the distribution server 10 to users of cellular phones 100, 102 and 104.

[0046] It is to be noted that, in the following description, notation {Y}X indicates that data Y is encrypted so that the data can be decrypted with a decryption key X.  
15

[0047] Furthermore, copyright concerning the content data or additional information Dc-inf as plaintext information concerned with server access or the like is distributed from the distribution server 10 together with the encrypted  
20 content data. In addition, as license, the license key Kc, and license ID which is a control code to specify distribution of the license key or the like from the distribution server 10 are exchanged between the distribution server 10 and the cellular phones 100, 102 and  
25 104. Furthermore, examples of the license include access control information ACm which is generated based on license purchase conditions AC including information such as a

content ID as a code to identify the content data Dc, a license number and a functional limitation determined in response to designation from a user side and which is information concerning a restriction on an access to the license in a recording device (a memory card); and reproduction control information ACp which is control information concerning reproduction in a data reproduction terminal.

[0048] Specifically, the access control information ACm is control information in a case where the license or the license key is output from the memory card, and includes limiting information concerning the number of reproducible times (the number of times to output the license key for the reproduction) and movement and duplicate of the license and the like.

[0049] The reproduction control information ACp is information which limits the reproduction, after a content reproduction circuit to reproduce the encrypted content data has received the license key. As shown in FIG. 3, the reproduction control information ACp includes flags FG1 to FG5 as reproduction limiting flags. The flag FG1 indicates reproduction speed change prohibition, the flag FG2 indicates whether or not edition is permitted, the flag FG3 indicates whether or not a region code is designated, the flag FG4 indicates whether or not a reproduction start date is designated, and the flag FG5 indicates whether or not a reproduction end date is designated. The reproduction

control information ACp further includes the corresponding region code in a case where the region code is designated, the corresponding reproduction start date in a case where the reproduction start date is designated, and the  
5 corresponding reproduction end date in a case where the reproduction end date is designated.

[0050] That is, the reproduction control information ACp includes an area 1 where the flags FG1 to FG5 are stored and an area 2 where actual data corresponding to the flags FG3  
10 to FG5 is stored. The area 2 includes areas 21 to 23. In a case where the flag FG3 indicates that the region code is designated, in the area 21, a region code indicating a region where the encrypted content data can be reproduced is stored. In the area 22, the reproduction start date of the  
15 encrypted content data is stored in a case where the flag FG4 indicates that the reproduction start date is designated. In the area 23, the reproduction end date of the encrypted content data is stored in a case where the flag FG5 indicates that the reproduction end date is designated.

[0051] In the flags FG1 to FG5, "1" or "0" is stored. When the flag indicates "1", it is meant that the flag is active and that a limitation due to a reproducing limitation corresponding to the flag is imposed. When the flag indicates "0", it is meant that the flag is negative and  
25 that any limitation due to the reproducing limitation corresponding to the flag is not imposed. Specifically, when "1" is stored in the flag FG1, the change prohibition

of the reproduction speed is meant. When "0" is stored, it is meant that the reproduction speed may be changed. When "1" is stored in the flag FG2, the permission of the edition is meant. When "0" is stored, the prohibition of the edition is meant. Furthermore, when "1" is stored in the flag FG3, it is meant that the region code capable of reproducing the encrypted content data is designated. When "0" is stored, it is meant that the region code capable of reproducing the encrypted content data is not designated, that is, all the areas are designated. In addition, when "1" is stored in the flag FG4, it is meant that the reproduction start date when the reproduction of the encrypted content data can be started is designated. When "0" is stored, it is meant that the reproduction start date when the reproduction of the encrypted content data can be started is not designated. Moreover, when "1" is stored in the flag FG5, it is meant that the reproduction end date when the encrypted content data cannot be reproduced any more is designated. When "0" is stored, it is meant that the reproduction end date when the encrypted content data cannot be reproduced any more is not designated.

[0052] Therefore, the reproduction circuit of the encrypted content data searches for the flags FG1 to FG5 of the reproduction control information ACp. Moreover, the reproduction circuit reproduces the encrypted content data without changing the speed in a case where "1" is stored in the flag FG1, and changes the speed to reproduce the

encrypted content data in a case where "0" is not stored.

The reproduction circuit edits the encrypted content data in response to an instruction from a user in a case where "1"

is stored in the flag FG2, and does not edit the encrypted

5 content data in a case where "0" is stored. Furthermore,

the reproduction circuit judges whether or not a region

where the encrypted content data is to be reproduced is a

region stored in the area 21 in a case where "1" is stored

in the flag FG3, reproduces the encrypted content data in a

10 case where it is judged that the region where the encrypted content data is to be reproduced is the region stored in the

area 21, and does not reproduce the encrypted content data

in a case where the region is a region other than the region

stored in the area 21 and the encrypted content data is to

15 be reproduced. Moreover, the reproduction circuit

reproduces the encrypted content data without judging

whether or not the region where the encrypted content data

is to be reproduced is the region stored in the area, in a

case where "0" is stored in the flag FG3.

20 [0053] Moreover, the reproduction circuit refers to the

reproduction start date stored in the area 22 in a case

where "1" is stored in the flag FG4, reproduces the

encrypted content data in a case where the reproduction

start date is reached, and does not reproduce the encrypted

25 content data in a case where the reproduction start date is

not reached. Furthermore, the reproduction circuit refers

to the reproduction end date stored in the area 23 in a case

where "1" is stored in the flag FG5, ends the reproduction of the encrypted content data in a case where the reproduction end date is reached, and continues the reproduction of the encrypted content data in a case where the reproduction end date is not reached.

[0054] It is to be noted that, in the present invention, either or the reproduction start date and the reproduction end date is designated in some case. That is, there is a case where the only reproduction start date is designated and the reproduction end date is not designated or a case where the reproduction start date is not designated and the reproduction end date is designated. In the former case, the reproduction end date is not stored in the area 23. In the latter case, the reproduction start date is not stored in the area 22.

[0055] In the present invention, especially, the reproduction start date or the reproduction end date is set to the reproduction control information ACp, and time of the reproduction of the encrypted content data is limited using the reproduction start date or the reproduction end date.

It is indicated that the areas 21 to 23 constituting the area 2 are constantly secured, but the areas may be omitted at a time when the corresponding flags FG3 to FG5 are negative or "0".

図1

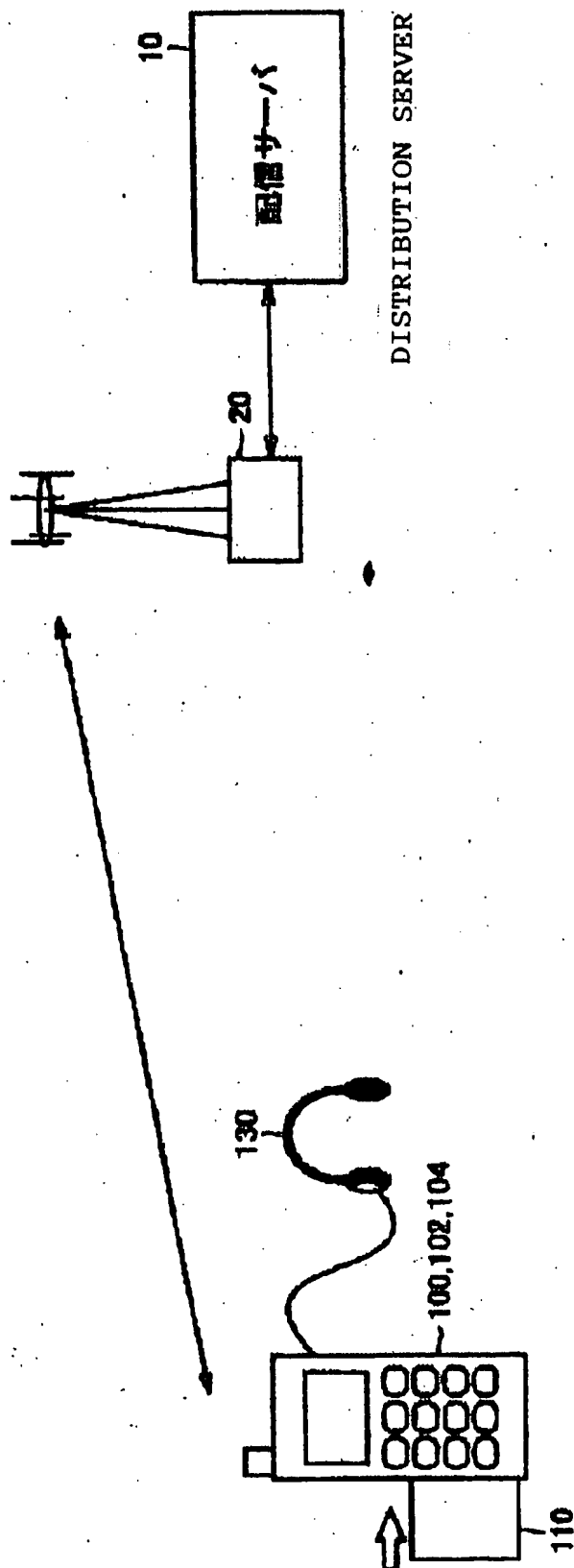




FIG. 2

| Symbol     | Type                   | Attribute            | Characteristics   |
|------------|------------------------|----------------------|---|
| Do         | Content data           | Inherent in contents | Ex.: Music data, reading data, teaching material data, image data, encrypted content data which can be decrypted with Kc and which is stored as {Dc}Kc and which is retained in memory card |
| Dc-inf     | Additional information | Inherent in contents | Plaintext data accompanying Dc  |
| Ko         | License                | Inherent in contents | License<br>Decryption key to decrypt encrypted content data   |
| ACm/ACp    | License                | Inherent in contents | Limit information<br>Limitation matters concerning reproduction and handling of license   |
| Content ID | License                | Inherent in contents | Control code to specify contents  |
| License ID | License                | Inherent in contents | Control code to specify license   |
| License    | License                | Inherent in license  | Generic term of Kc + ACm + ACp + Content ID + License ID  |

FIG. 3

ACp flag

Reproduction limiting flag

FG1: Reproduction speed change prohibition

FG2: Whether or not edition is permitted

FG3: Whether or not region code is designated

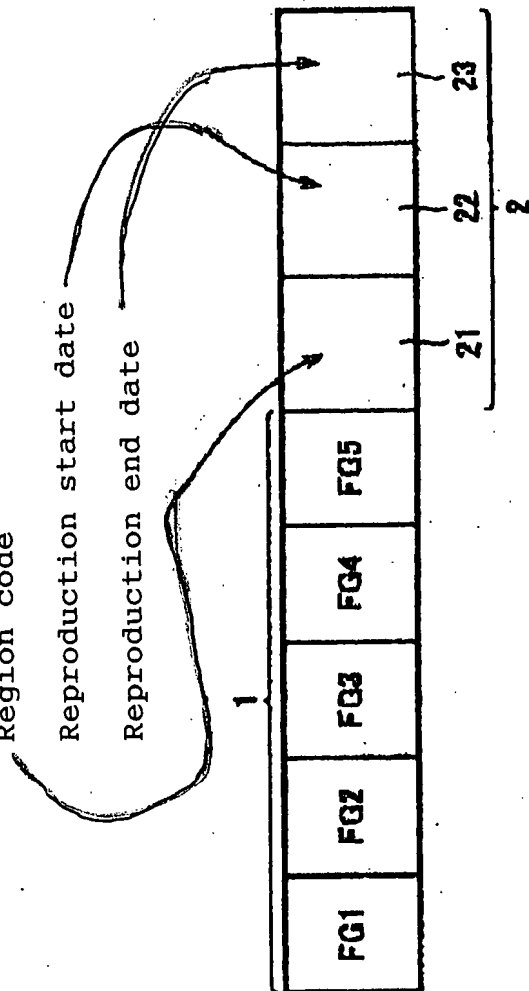
FG4: Whether or not reproduction start date is designated

FG5: Whether or not reproduction end date is designated

Region code

Reproduction start date

Reproduction end date



(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-366442

(P2002-366442A)

(43) 公開日 平成14年12月20日 (2002. 12. 20)

| (51) Int.Cl. <sup>7</sup> | 識別記号  | F I           | テーマコード* (参考) |           |
|---------------------------|-------|---------------|--------------|-----------|
| G 0 6 F 12/14             | 3 2 0 | G 0 6 F 12/14 | 3 2 0 F      | 5 B 0 1 7 |
|                           |       |               | 3 2 0 B      | 5 B 0 3 5 |
| G 0 6 K 19/073            |       | H 0 4 M 11/00 | 3 0 2        | 5 C 0 5 2 |
| H 0 4 L 9/08              |       | H 0 4 N 5/907 | B            | 5 C 0 5 3 |
| H 0 4 M 11/00             | 3 0 2 | G 0 6 K 19/00 | P            | 5 C 0 6 4 |

審査請求 未請求 請求項の数15 OL (全 33 頁) 最終頁に続く

(21) 出願番号 特願2001-175036(P2001-175036)

(22) 出願日 平成13年6月11日 (2001. 6. 11)

(71) 出願人 000001889

三洋電機株式会社

大阪府守口市京阪本通2丁目5番5号

(72) 発明者 堀 吉宏

大阪府守口市京阪本通2丁目5番5号 三

洋電機株式会社内

(74) 代理人 100064746

弁理士 深見 久郎 (外3名)

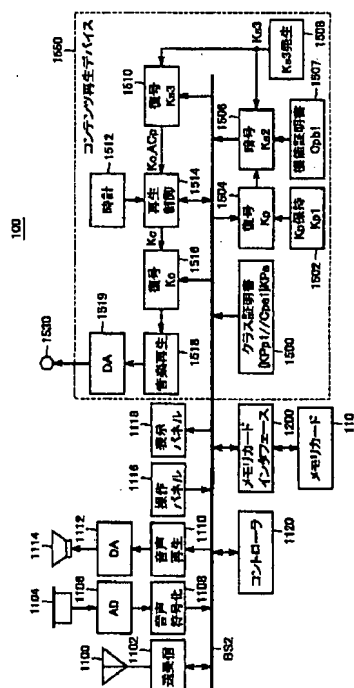
最終頁に続く

(54) 【発明の名称】 データ端末装置およびデータ記録装置

(57) 【要約】

【課題】 再生端末で制御できない再生制御を受ける暗号化コンテンツデータや再生端末で再生できない暗号化コンテンツデータに対するライセンス鍵を端末装置に提供しないデータ記録装置およびそれに対応したデータ端末装置を提供する。

【解決手段】 携帯電話機100は、機能証明書保持部1507を備え、機能証明書Cpb1をメモリカード110へ送信する。そして、機能証明書によって証明される機能が再生制御情報ACPによって制限される機能に対応しているとき、携帯電話機100は、暗号化コンテンツデータ{Dc} Kcを復号するためのライセンス鍵Kcと再生制御情報ACPをメモリカード110から取得する。再生制御部1514は、時計1512からの時間情報と再生制御情報ACPに含まれる再生期限とに基づいて暗号化コンテンツデータ{Dc} Kcの再生の可否を判断する。



## 【特許請求の範囲】

【請求項 1】 暗号化コンテンツデータと、前記暗号化コンテンツデータを復号するためのライセンス鍵を含むライセンスとをデータ記録装置から取得して前記暗号化コンテンツデータを復号および再生するデータ端末装置であって、

前記データ記録装置との間のデータのやり取りを制御するインタフェースと、

前記暗号化コンテンツデータを前記ライセンス鍵によって復号および再生するコンテンツ再生手段と、

前記コンテンツ再生手段における再生機能を証明する機能証明書を保持する機能証明書保持部と、

指示を入力するためのキー操作部と、

制御手段とを備え、

前記制御手段は、前記キー操作部を介して入力された前記暗号化コンテンツデータの再生要求に応じて前記機能証明書を前記インタフェースを介して前記データ記録装置へ送信し、前記機能証明書によって証明された機能が前記ライセンスに含まれる再生制限情報により制限しようとする機能に対応しているとき、前記インタフェースを介して前記データ記録装置から前記暗号化コンテンツデータおよび前記ライセンスを受信し、その受信した暗号化コンテンツデータおよびライセンスを前記コンテンツ再生手段に与える、データ端末装置。

【請求項 2】 データを前記データ記録装置と送受信するときのセキュリティレベルを証明するクラス証明書を保持するクラス証明書保持部をさらに備え、

前記制御手段は、前記再生要求に応じて前記クラス証明書を前記インタフェースを介して前記データ記録装置へ送信し、前記データ記録装置において前記クラス証明書が認証されると、前記機能証明書を前記データ記録装置へ送信する、請求項 1 に記載のデータ端末装置。

【請求項 3】 前記機能証明書保持部は、前記クラス証明書に含まれる公開暗号鍵によって復号可能な暗号化された機能証明書を保持する、請求項 2 に記載のデータ端末装置。

【請求項 4】 前記制御手段は、前記機能証明書を前記クラス証明書と同時に前記データ記録装置へ送信する、請求項 3 に記載のデータ端末装置。

【請求項 5】 前記データ記録装置との通信を特定するためのセッション鍵を生成するセッション鍵生成手段と、

前記セッション鍵によってデータを暗号化する暗号処理手段と、

前記セッション鍵によって暗号化された暗号化データを復号する復号処理手段とをさらに備え、

前記暗号化コンテンツデータおよび前記ライセンスを前記データ記録装置から取得するとき、

前記セッション鍵生成手段は、前記データ記録装置との通信を特定するための第 1 のセッション鍵を生成し、

前記暗号処理手段は、前記機能証明書および前記第 1 のセッション鍵を、前記データ記録装置から受取った第 2 のセッション鍵によって暗号化し、

前記制御手段は、前記第 2 のセッション鍵によって暗号化された前記機能証明書および前記第 1 のセッション鍵を前記インタフェースを介して前記データ記録装置へ送信する、請求項 2 から請求項 4 のいずれか 1 項に記載のデータ端末装置。

【請求項 6】 前記制御手段は、さらに、前記第 1 のセッション鍵によって暗号化された前記再生制限情報および前記ライセンス鍵を前記データ記録装置から受信して前記復号処理手段に与え、前記復号処理手段により復号された前記再生制限情報によって前記暗号化コンテンツデータの再生が制限されていないとき前記暗号化コンテンツデータおよび前記ライセンス鍵を前記コンテンツ再生手段に与える、請求項 5 に記載のデータ端末装置。

【請求項 7】 リアルタイムに日時情報を更新する時計部をさらに備え、

前記再生制限情報は、前記暗号化コンテンツデータの再生期間を制限する期間制限情報を含み、

前記制御手段は、前記時計部からの日時情報と前記期間制限情報とに基づいて前記暗号化コンテンツデータの再生期間内か否かを判定する、請求項 6 に記載のデータ端末装置。

【請求項 8】 暗号化コンテンツデータと、前記暗号化コンテンツデータを復号するためのライセンス鍵を含むライセンスとを記録するデータ記録装置であって、前記暗号化コンテンツデータおよび前記ライセンスを記憶する記憶手段と、

前記暗号化コンテンツデータを前記ライセンスによって復号および再生するデータ再生装置との間でデータのやり取りを行なうインタフェースと、

制御手段とを備え、

前記制御手段は、前記データ再生装置の機能を証明する機能証明書を前記インタフェースを介して受取り、その受取った機能証明書によって証明された機能が前記ライセンスに含まれる再生制限情報により制限しようとする機能に対応しているとき、前記暗号化コンテンツデータおよび前記ライセンスを前記記憶手段から読出して前記インタフェースを介して前記データ再生装置へ送信する、データ記録装置。

【請求項 9】 前記データ再生装置に固有な公開暗号鍵によって暗号化されたデータを秘密復号鍵によって復号する復号処理手段をさらに備え、

前記制御手段は、前記公開暗号鍵によって暗号化された機能証明書を前記インタフェースを介して受取り、前記暗号化された機能証明書を前記復号処理手段に与え、復号された機能証明書を前記復号処理手段から受取る、請求項 8 に記載のデータ記録装置。

【請求項 10】 公開認証鍵によって暗号化されたデー

タを前記公開認証鍵によって復号する第1の復号処理手段と、

前記データ再生装置に固有な公開暗号鍵によって暗号化されたデータを秘密復号鍵によって復号する第2の復号処理手段とをさらに備え、

前記制御手段は、前記公開認証鍵によって復号可能な暗号化されたクラス証明書と、前記公開暗号鍵によって復号可能な暗号化された機能証明書とを前記インタフェースを介して同時に受取り、前記暗号化されたクラス証明書 10 前記第1の復号処理手段に与え、前記暗号化された機能証明書を前記第2の復号処理手段に与え、復号されたクラス証明書および機能証明書を受取る、請求項8に記載のデータ記録装置。

【請求項11】 前記データ再生装置との通信を特定するためのセッション鍵を生成するセッション鍵生成手段と、

前記セッション鍵によって暗号化されたデータを復号するもう1つの復号処理手段と、

前記データ再生装置に固有な公開暗号鍵によってデータを暗号化する暗号処理手段とをさらに備え、 20

前記機能証明書を受信するとき、

前記セッション鍵生成手段は、前記データ再生装置との通信を特定するための第1のセッション鍵を生成し、

前記暗号処理手段は、前記公開暗号鍵によって前記第1のセッション鍵を暗号化し、

前記制御手段は、前記公開暗号鍵によって暗号化された第1のセッション鍵を前記インタフェースを介して前記データ再生装置へ送信し、前記第1のセッション鍵によって暗号化された機能証明書を前記インタフェースを介して受信して前記もう1つの復号処理手段に与え、復号 30 された機能証明書を前記もう1つの復号処理手段から受取り、

前記もう1つの復号処理手段は、前記暗号化された機能証明書を前記第1のセッション鍵によって復号する、請求項8から請求項10のいずれか1項に記載のデータ記録装置。

【請求項12】 前記セッション鍵によってデータを暗号化するもう1つの暗号処理手段をさらに備え、

前記制御手段は、前記機能証明書によって証明された機能が前記ライセンスに含まれる再生制限情報により制限しようとする機能に対応していると判断すると、前記記憶手段から読出した前記ライセンス鍵および前記再生制限情報を前記もう1つの暗号処理手段に与え、前記データ再生装置において生成された第2のセッション鍵によって暗号化されたライセンス鍵および再生制限情報を前記インタフェースを介して前記データ再生装置へ送信し、 40

前記もう1つの暗号処理手段は、前記第2のセッション鍵によって前記ライセンス鍵および前記再生制限情報を暗号化する、請求項11に記載のデータ記録装置。 50

【請求項13】 前記制御手段は、前記データ再生装置が前記機能証明書を保持しないときデフォルト値を前記機能証明書として受理する、請求項8から請求項12のいずれか1項に記載のデータ記録装置。

【請求項14】 前記再生制限情報は、前記暗号化コンテンツデータの再生を開始できる再生開始日時と、

前記暗号化コンテンツデータの再生ができなくなる再生終了日時とのいずれか一方を少なくとも含む、請求項8から請求項13のいずれか1項に記載のデータ記録装置。

【請求項15】 前記再生制限情報は、前記暗号化コンテンツデータを再生可能な地域を示す地域コードをさらに含む、請求項14に記載のデータ記録装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムを用いて取得された暗号化データを復号および再生する際に、暗号化データの再生制限情報の内容に応じた暗号化データの再生を実現するデータ端末装置およびデータ記録装置に関するものである。

【0002】

【従来の技術】近年、インターネット等のデジタル情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【0003】このようなデジタル情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【0004】したがって、このようなデジタル情報通信網上において音楽データや画像データ等の著作権者の権利が存在するコンテンツが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【0005】一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【0006】ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したCD（コンパクトディスク）については、CDから光磁気ディスク（MD等）への音楽デー

タのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

【0007】しかも、CDからMDへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なMDからさらに他のMDに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【0008】このような事情からも、音楽データや画像データ等のコンテンツデータをデジタル情報通信網を通じて公衆に配信することは、それ自身が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【0009】この場合、デジタル情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【0010】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、暗号化コンテンツデータやライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【0011】最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテンツデータをメモリカードに送信する。そして、メモリカードは、受信したライセンス鍵と暗号化コンテンツデータをメモリカードに記録する。

【0012】そして、メモリカードに記録した暗号化コンテンツデータを再生するときは、メモリカードを携帯電話機に装着する。携帯電話機は、通常の電話機能の他にメモリカードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。

【0013】このように、携帯電話機のユーザは、ダウンロード端末としての携帯電話機を用いて暗号化コンテンツデータと暗号化コンテンツデータを再生するために必要なライセンス鍵を含むライセンスを配信サーバから受信し、その暗号化コンテンツデータを再生することができる。そして、暗号化コンテンツデータを復号および再生するために必要なライセンスは、ライセンス鍵の他に暗号化コンテンツデータの再生に対して制限を加える再生制限情報を含み、暗号化コンテンツデータを再生するデータ端末装置としての携帯電話機は、この再生制限情報に従って暗号化コンテンツデータの再生の際に制限を加える。

【0014】

【発明が解決しようとする課題】しかし、このようなシステムにおいては、データ記録装置であるメモリカードが中心となってユーザ側でのライセンスの管理を行なっているにも拘わらず、ライセンス鍵を安全に管理しているデータ記録装置は、再生端末による制限が必ず実施されているかを判断することができないという問題があった。

【0015】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、再生端末で制御できない再生制御を受ける暗号化コンテンツデータや再生端末で再生できない暗号化コンテンツデータに対するライセンス鍵を端末装置に提供しないデータ記録装置およびそれに対応したデータ端末装置を提供することである。

【0016】

【課題を解決するための手段】この発明によれば、データ端末装置は、暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を含むライセンスとをデータ記録装置から取得して暗号化コンテンツデータを復号および再生するデータ端末装置であって、データ記録装置との間のデータのやり取りを制御するインタフェースと、暗号化コンテンツデータをライセンス鍵によって復号および再生するコンテンツ再生手段と、コンテンツ再生手段における再生機能を証明する機能証明書を保持する機能証明書保持部と、指示を入力するためのキー操作部と、制御手段とを備え、制御手段は、キー操作部を介して入力された暗号化コンテンツデータの再生要求に応じて機能証明書をインタフェースを介してデータ記録装置へ送信し、機能証明書によって証明された機能がライセンスに含まれる再生制限情報により制限しようとする機能に対応しているとき、インタフェースを介してデータ記録装置から暗号化コンテンツデータおよびライセンスを受信し、その受信した暗号化コンテンツデータおよびライセンスをコンテンツ再生手段に与える。

【0017】好ましくは、データ端末装置は、データを前記データ記録装置と送受信するときのセキュリティレ

10

20

30

40

50

ベルを証明するクラス証明書を保持するクラス証明書保持部をさらに備え、制御手段は、再生要求に応じてクラス証明書をインタフェースを介してデータ記録装置へ送信し、データ記録装置においてクラス証明書が認証されると、機能証明書を前記データ記録装置へ送信する。

【0018】好ましくは、機能証明書保持部は、クラス証明書に含まれる公開暗号鍵によって復号可能な暗号化された機能証明書を保持する。

【0019】好ましくは、制御手段は、機能証明書をクラス証明書と同時にデータ記録装置へ送信する。

【0020】好ましくは、データ端末装置は、データ記録装置との通信を特定するためのセッション鍵を生成するセッション鍵生成手段と、セッション鍵によってデータを暗号化する暗号処理手段と、セッション鍵によって暗号化された暗号化データを復号する復号処理手段とをさらに備え、暗号化コンテンツデータおよびライセンスをデータ記録装置から取得するとき、セッション鍵生成手段は、データ記録装置との通信を特定するための第1のセッション鍵を生成し、暗号処理手段は、機能証明書および第1のセッション鍵を、データ記録装置から受取った第2のセッション鍵によって暗号化し、制御手段は、第2のセッション鍵によって暗号化された機能証明書および第1のセッション鍵をインタフェースを介してデータ記録装置へ送信する。

【0021】好ましくは、制御手段は、さらに、第1のセッション鍵によって暗号化された再生制限情報およびライセンス鍵をデータ記録装置から受信して復号処理手段に与え、復号処理手段により復号された再生制限情報によって暗号化コンテンツデータの再生が制限されていないとき暗号化コンテンツデータおよびライセンス鍵をコンテンツ再生手段に与える。

【0022】好ましくは、データ端末装置は、リアルタイムに日時情報を更新する時計部をさらに備え、再生制限情報は、暗号化コンテンツデータの再生期間を制限する期間制限情報を含み、制御手段は、時計部からの日時情報と期間制限情報とに基づいて暗号化コンテンツデータの再生期間内可否かを判定する。

【0023】また、この発明によれば、データ記録装置は、暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を含むライセンスとを記録するデータ記録装置であって、暗号化コンテンツデータおよびライセンスを記憶する記憶手段と、暗号化コンテンツデータをライセンスによって復号および再生するデータ再生装置との間でデータのやり取りを行なうインタフェースと、制御手段とを備え、制御手段は、データ再生装置の機能を証明する機能証明書をインタフェースを介して受取り、その受取った機能証明書によって証明された機能がライセンスに含まれる再生制限情報により制限しようとする機能に対応しているとき、暗号化コンテンツデータおよびライセンスを記憶手段から読出し

てインタフェースを介してデータ再生装置へ送信する。

【0024】好ましくは、データ記録装置は、データ再生装置に固有な公開暗号鍵によって暗号化されたデータを秘密復号鍵によって復号する復号処理手段をさらに備え、制御手段は、公開暗号鍵によって暗号化された機能証明書をインタフェースを介して受取り、暗号化された機能証明書を復号処理手段に与え、復号された機能証明書を復号処理手段から受取る。

【0025】好ましくは、データ記録装置は、公開認証鍵によって暗号化されたデータを公開認証鍵によって復号する第1の復号処理手段と、データ再生装置に固有な公開暗号鍵によって暗号化されたデータを秘密復号鍵によって復号する第2の復号処理手段とをさらに備え、制御手段は、公開認証鍵によって復号可能な暗号化されたクラス証明書と、公開暗号鍵によって暗号化された機能証明書をインタフェースを介して同時に受取り、暗号化されたクラス証明書を第1の復号処理手段に与え、暗号化された機能証明書を第2の復号処理手段に与え、復号されたクラス証明書および機能証明書を受取る。

【0026】好ましくは、データ記録装置は、データ再生装置との通信を特定するためのセッション鍵を生成するセッション鍵生成手段と、セッション鍵によって暗号化されたデータを復号するもう1つの復号処理手段と、データ再生装置に固有な公開暗号鍵によってデータを暗号化する暗号処理手段とをさらに備え、機能証明書を受信するとき、セッション鍵生成手段は、データ再生装置との通信を特定するための第1のセッション鍵を生成し、暗号処理手段は、公開暗号鍵によって第1のセッション鍵を暗号化し、制御手段は、公開暗号鍵によって暗号化された第1のセッション鍵をインタフェースを介してデータ再生装置へ送信し、第1のセッション鍵によって暗号化された機能証明書をインタフェースを介して受信してもう1つの復号処理手段に与え、復号された機能証明書をもう1つの復号処理手段から受取り、もう1つの復号処理手段は、暗号化された機能証明書を第1のセッション鍵によって復号する。

【0027】好ましくは、セッション鍵によってデータを暗号化するもう1つの暗号処理手段をさらに備え、制御手段は、機能証明書によって証明された機能がライセンスに含まれる再生制限情報により制限しようとする機能に対応していると判断すると、記憶手段から読出したライセンス鍵および再生制限情報をもう1つの暗号処理手段に与え、データ再生装置において生成された第2のセッション鍵によって暗号化されたライセンス鍵および再生制限情報をインタフェースを介してデータ再生装置へ送信し、もう1つの暗号処理手段は、第2のセッション鍵によってライセンス鍵および再生制限情報を暗号化する。

【0028】好ましくは、制御手段は、データ再生装置が機能証明書を保持しないときデフォルト値を機能証明

10

20

30

40

50

審として受理する。

【0029】好ましくは、再生制限情報は、暗号化コンテンツデータの再生を開始できる再生開始日時と、暗号化コンテンツデータの再生ができなくなる再生終了日時とのいずれか一方を少なくとも含む。

【0030】好ましくは、再生制限情報は、暗号化コンテンツデータを再生可能な地域を示す地域コードをさらに含む。

【0031】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【0032】【実施の形態1】図1は、本発明によるデータ記録装置が暗号化コンテンツデータおよび暗号化コンテンツデータを復号するためのライセンスを取得するデータ配信システムの全体構成を概念的に説明するための概略図である。

【0033】なお、以下では携帯電話網を介して音楽データをユーザの携帯電話機に装着されたメモリカード110に配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画データ等を配信する場合においても適用することが可能なものである。

【0034】図1を参照して、配信キャリア20は、自己の携帯電話網を通じて得た、ユーザからの配信要求（配信リクエスト）を配信サーバ10に中継する。音楽データを管理する配信サーバ10は、データ配信を求めてアクセスして来た携帯電話ユーザの携帯電話機100、102、104に装着されたメモリカード110が正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行ない、正当なメモリカードに対して著作権を保護するために所定の暗号方式により音楽データ（以下、コンテンツデータと呼ぶ）を暗号化した上で、データを配信するための配信キャリア20である携帯電話会社に、このような暗号化コンテンツデータおよび暗号化コンテンツデータを再生するために必要な情報として暗号化コンテンツデータを復号するためのライセンス鍵を含むライセンスを与える。

【0035】配信キャリア20は、自己の携帯電話網を通じて配信要求を送信した携帯電話機100、102、104に装着されたメモリカード110に対して、携帯電話網および携帯電話機100、102、104を介して暗号化コンテンツデータとライセンスとを配信する。

【0036】図1においては、たとえば携帯電話ユーザの携帯電話機100、102、104には、着脱可能なメモリカード110が装着される構成となっている。メモリカード110は、携帯電話機100、102、104により受信された暗号化コンテンツデータを受取り、

著作権を保護するために行なわれた暗号化を復号した上で、携帯電話機100、102、104に含まれる音楽再生部（図示せず）に与える。

【0037】さらに、たとえば携帯電話ユーザは、携帯電話機100、102、104に接続したヘッドホン130等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

【0038】このような構成とすることで、まず、メモリカード110を利用しないと、配信サーバ10からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【0039】しかも、配信キャリア20において、たとえば1曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア20が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【0040】したがって、図1に示すデータ配信システムにおいては、携帯電話機100に装着されたメモリカード110は、携帯電話網を介して配信サーバ10から暗号化コンテンツデータおよびライセンスを受信することができる。

【0041】図1に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話機のユーザ側で再生可能とするためにシステム上必要とされるのは、第1には、通信におけるライセンスを配信するための方式であり、さらに第2には、コンテンツデータを暗号化する方式そのものであり、さらに、第3には、このような再生可能な状態でのコンテンツデータの無断コピーを防止するための著作権保護を実現する構成である。

【0042】本発明の実施の形態においては、特に、配信、および再生の各処理の発生時において、これらの暗号化コンテンツデータを再生するために必要なライセンスの移動先に対する認証およびチェック機能を充実させ、非認証の記録装置およびデータ再生端末（暗号化コンテンツデータを復号して再生できる再生端末を携帯電話機とも言う。以下同じ）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【0043】なお、以下の説明においては、配信サーバ10から、各携帯電話機に暗号化コンテンツデータまたはそのライセンスを伝送する処理を「配信」と称することとする。

【0044】図2は、図1に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【0045】まず、配信サーバ10より配信されるデータについて説明する。Dcは、音楽データ等のコンテンツデータである。コンテンツデータDcは、ライセンス



鍵Kcで復号可能な暗号化が施される。ライセンス鍵Kcによって復号可能な暗号化が施された暗号化コンテンツデータ{Dc}Kcがこの形式で配信サーバ10より携帯電話機100、102、104のユーザに配布される。

【0046】なお、以下においては、{Y}Xという表記は、データYを、復号鍵Xにより復号可能な暗号化を施したことを示すものとする。

【0047】さらに、配信サーバ10からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Dc-infが配布される。また、ライセンスとして、ライセンス鍵Kc、配信サーバ10からのライセンスIDが配信サーバ10と携帯電話機100、102、104との間でやり取りされる。さらに、ライセンスとしては、コンテンツデータDcを識別するためのコードであるコンテンツIDや、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ACに基づいて生成される、記録装置(メモリカード)におけるライセンスのアクセスに対する制限に関する情報であるアクセス制御情報ACmおよびデータ再生端末における再生に関する制御情報である再生制御情報ACp等が存在する。

【0048】具体的には、アクセス制御情報ACmは、メモリカードからのライセンスまたはライセンス鍵を外部に出力するに当たっての制御情報であり、再生可能回数(再生のためにライセンス鍵を出力する回数)、ライセンスの移動・複製に関する制限情報などがある。

【0049】再生制御情報ACpは、暗号化コンテンツデータを再生するためにコンテンツ再生回路がライセンス鍵を受取った後に、再生を制限する情報である。図3を参照して、再生制御情報ACpは、再生制限フラグとしてフラグFG1~FG5を含む。フラグFG1は、再生速度変更禁止を示し、フラグFG2は、編集可否を示し、フラグFG3は、地域コードの指定有無を示し、フラグFG4は、再生開始日時の指定有無を示し、フラグFG5は、再生終了日時の指定有無を示す。再生制御情報ACpは、さらに、地域コードの指定が有る場合、それに対応する地域コードと、再生開始日時の指定が有る場合、それに対応する再生開始日時と、再生終了日時の指定がある場合、それに対応する再生終了日時を含む。

【0050】すなわち、再生制御情報ACpは、フラグFG1~FG5が格納された領域1と、フラグFG3~FG5に対応する実データが格納された領域2とから成る。領域2は、領域21~23から成る。領域21は、フラグFG3において地域コードの指定がある場合に、暗号化コンテンツデータの再生が可能な地域を示す地域コードが格納される。領域22は、フラグFG4におい

て再生開始日時の指定がある場合に、暗号化コンテンツデータの再生開始日時が格納される。領域23は、フラグFG5において再生終了日時の指定がある場合に、暗号化コンテンツデータの再生終了日時が格納される。

【0051】フラグFG1~FG5には、「1」または「0」が格納される。フラグが「1」の場合には、そのフラグはアクティブであって、そのフラグに対応した再生制限による制限を受けることを意味し、フラグが「0」の場合には、そのフラグがネガティブであって、そのフラグに対応した再生制限による制限を受けないことを意味する。具体的には、フラグFG1に「1」が格納された場合、再生速度の変更禁止を意味し、「0」が格納された場合、再生速度を変更しても良いことを意味する。また、フラグFG2に「1」が格納された場合、編集の許可を意味し、「0」が格納された場合、編集の禁止を意味する。さらに、フラグFG3に「1」が格納された場合、暗号化コンテンツデータを再生できる地域コードの指定が有ることを意味し、「0」が格納された場合、暗号化コンテンツデータを再生できる地域コードの指定が無い、すなわち、全領域指定であることを意味する。また、さらに、フラグFG4に「1」が格納された場合、暗号化コンテンツデータの再生を開始できる再生開始日時の指定が有ることを意味し、「0」が格納された場合、暗号化コンテンツデータの再生を開始できる再生開始日時の指定が無いことを意味する。また、さらに、フラグFG5に「1」が格納された場合、暗号化コンテンツデータの再生ができなくなる再生終了日時の指定が有ることを意味し、「0」が格納された場合、暗号化コンテンツデータの再生ができなくなる再生終了日時の指定が無いことを意味する。

【0052】したがって、暗号化コンテンツデータの再生回路は、再生制御情報ACpのフラグFG1~FG5を検索する。そして、再生回路は、フラグFG1において「1」が格納されていれば、速度を変更せずに暗号化コンテンツデータを再生し、「0」が格納されていなければ速度を変更して暗号化コンテンツデータを再生する。また、再生回路は、フラグFG2に「1」が格納されていれば、ユーザからの指示により暗号化コンテンツデータの編集を行ない、「0」が格納されていれば暗号化コンテンツデータの編集を行なわない。さらに、再生回路は、フラグFG3に「1」が格納されていれば、暗号化コンテンツデータを再生しようとする地域が領域21に格納された地域であるか否かを判定し、暗号化コンテンツデータを再生しようとする地域が領域21に格納された地域であれば暗号化コンテンツデータの再生を行ない、領域21に格納された地域以外で暗号化コンテンツデータを再生しようとしているときは暗号化コンテンツデータの再生を行なわない。そして、再生回路は、フラグFG3に「0」が格納されていれば、暗号化コンテンツデータを再生しようとしている地域の判定を行なわ

ずに暗号化コンテンツデータの再生を行なう。

【0053】また、さらに、再生回路は、フラグFG4に「1」が格納されていれば、領域22に格納された再生開始日時を参照し、その再生開始日時に違っていれば暗号化コンテンツデータの再生を行ない、再生開始日時に違っていなければ暗号化コンテンツデータの再生を行なわない。また、さらに、再生回路は、フラグFG5に「1」が格納されていれば、領域23に格納された再生終了日時を参照し、その再生終了日時に違っていれば暗号化コンテンツデータの再生を終了し、再生終了日時に違っていなければ暗号化コンテンツデータの再生を続行する。

【0054】なお、本発明においては、再生開始日時および再生終了日時のうちいずれか一方のみが指定される場合もある。すなわち、再生開始日時のみが指定され、再生終了日時が指定されていない場合、または再生開始日時が指定されず、再生終了日時が指定されている場合がある。前者の場合、領域23には再生終了日時が格納されず、後者の場合、領域22には再生開始日時が格納されない。

【0055】本発明においては、特に、再生開始日時または再生終了日時を再生制御情報ACpに設定し、再生開始日時または再生終了日時を用いて暗号化コンテンツデータの再生を時間的に制限する。また、領域2を構成する領域21～23は、常に確保されているように示されているが、それぞれに対応するフラグFG3～FG5がネガティブ「0」の時には省略するように構成してもよい。

【0056】再び、図2を参照して、ライセンスIDと、コンテンツIDと、ライセンス鍵Kcと、アクセス制御情報ACmと、再生制御情報ACpとを併せて、以後、ライセンスと総称することとする。

【0057】また、以降では、簡単化のためアクセス制御情報ACmは、再生回数の制限を行なう制御情報である再生回数（0：再生不可、1～254：再生可能回数、255：制限無し）、ライセンスの移動および複製を制限する移動・複製フラグ（0：移動複製禁止、1：移動のみ可、2：移動複製可）の2項目とする。

【0058】図4は、図1に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を説明する図である。

【0059】データ再生端末内のコンテンツ再生デバイス、およびメモ리카ードには固有の公開暗号鍵Kp<sub>y</sub>およびKp<sub>m</sub>wがそれぞれ設けられ、公開暗号鍵Kp<sub>y</sub>およびKp<sub>m</sub>wはコンテンツ再生回路に固有の秘密復号鍵Kp<sub>y</sub>およびメモ리카ードに固有の秘密復号鍵Km<sub>w</sub>によってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、メモ리카ードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称し、これらの公開暗号鍵をクラス公開

暗号鍵、秘密復号鍵をクラス秘密復号鍵、クラス鍵を共有する単位をクラスと称する。クラスは、製造会社や製品の種類、製造時のロット等によって異なる。

【0060】また、コンテンツ再生デバイスのクラス証明書としてCp<sub>a</sub>yが設けられ、メモ리카ードのクラス証明書としてCm<sub>w</sub>が設けられる。これらのクラス証明書は、コンテンツ再生デバイス、およびメモ리카ードのクラスごとに異なる情報を有する。

【0061】さらに、コンテンツ再生デバイスの機能証明書としてCp<sub>b</sub>iが設けられる。この機能証明書は、コンテンツ再生デバイスが、再生制御情報ACpによって制限可能な機能を備えるか否かを示すものである。すなわち、再生制御情報ACpとして、再生開始日時または再生終了日時を設定した場合、コンテンツ再生デバイスは、暗号化コンテンツデータを再生する際の日時が、設定された再生開始日時または再生終了日時の条件を満たすか否かを判定する必要がある。そうすると、再生制御情報ACpとして再生開始日時または再生終了日時が設定されている暗号化コンテンツデータの再生が可能なコンテンツ再生デバイスは、時間を判定する機能を備えたコンテンツ再生デバイスである。したがって、コンテンツ再生デバイスのクラスごとに、時間の判定機能の有無が機能証明書Cp<sub>b</sub>iに記載されている。

【0062】これらのコンテンツ再生デバイスのクラス公開暗号鍵およびクラス証明書は、認証データ{Kp<sub>y</sub>//Cp<sub>a</sub>y}Kp<sub>a</sub>の形式で出荷時にコンテンツ再生デバイスに記録され、メモ리카ードのクラス公開暗号鍵およびクラス証明書は認証データ{Kp<sub>m</sub>w//Cm<sub>w</sub>}Kp<sub>a</sub>の形式で出荷時にメモ리카ードに記録される。また、機能証明書は、Cp<sub>b</sub>iまたは{Cp<sub>b</sub>i}Kp<sub>y</sub>の形式で出荷時にコンテンツ再生デバイスに記録される。後ほど詳細に説明するが、Kp<sub>a</sub>は配信システム全体で共通の公開認証鍵である。

【0063】以降では、説明を簡単にするために機能証明書は、再生制御情報ACpのフラグFG3～FG5によって示される地域コード、再生開始日時、再生終了日時についての対応の可否が記載され、フラグFG1、FG2に対応することはコンテンツ再生デバイスにとって標準の機能であるものとする。

【0064】また、メモ리카ード110内のデータ処理を管理するための鍵として、メモ리카ードという媒体ごとに設定される公開暗号鍵Kp<sub>m</sub>c<sub>x</sub>と、公開暗号鍵Kp<sub>m</sub>c<sub>x</sub>で暗号化されたデータを復号することが可能な秘密復号鍵Km<sub>c</sub>xとが存在する。これらのメモ리카ードごとに設定される公開暗号鍵および秘密復号鍵を総称して個別鍵と称し、公開暗号鍵Kp<sub>m</sub>c<sub>x</sub>を個別公開暗号鍵、秘密復号鍵Km<sub>c</sub>xを個別秘密復号鍵と称する。

【0065】ライセンスの配信および再生が行なわれるごとに配信サーバ10、携帯電話機100、102、104、およびメモ리카ード110において生成される共

通鍵Ks1~Ks3が用いられる。

【0066】ここで、共通鍵Ks1~Ks3は、配信サーバ、コンテンツ再生デバイスもしくはメモ리카ード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ks1~Ks3を「セッションキー」とも呼ぶこととする。

【0067】これらのセッションキーKs1~Ks3は、各セッションごとに固有の値を有することにより、配信サーバ、コンテンツ再生デバイス、およびメモ리카ードによって管理される。具体的には、セッションキーKs1は、配信サーバによって配信セッションごとに発生される。セッションキーKs2は、メモ리카ードによって配信セッションおよび再生セッションごとに発生し、セッションキーKs3は、コンテンツ再生デバイスにおいて再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行した上でライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【0068】図5は、図1に示した配信サーバ10の構成を示す概略ブロック図である。配信サーバ10は、コンテンツデータを所定の方式に従って暗号化したデータやコンテンツID等の配信情報を保持するための情報データベース304と、携帯電話機のユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース302と、情報データベース304に保持されたコンテンツデータのメニューを保持するメニューデータベース307と、ライセンスの配信ごとに生成され、かつ、ライセンスを特定するライセンスID等の配信に関するログを保持する配信記録データベース308と、情報データベース304、課金データベース302、メニューデータベース307、および配信記録データベース308からのデータをバスBS1を介して受取り、所定の処理を行なうためのデータ処理部310と、通信網を介して、配信キャリア20とデータ処理部310との間でデータ授受を行なうための通信装置350とを備える。

【0069】データ処理部310は、バスBS1上のデータに応じて、データ処理部310の動作を制御するための配信制御部315と、配信制御部315により制御されて、配信セッション時にセッションキーKs1を発生するためのセッションキー発生部316と、メモ리카ードから送られてきた認証のための認証データ{Kpmw/Cmw}KPaを復号するための公開認証鍵KPaを保持する認証鍵保持部313と、メモ리카ードから送られてきた認証のための認証データ{Kpmw/Cmw}KPaを通信装置350およびバスBS1を介して受けて、認証鍵保持部313からの公開認証鍵KPa

によって復号処理を行なう復号処理部312と、配信セッションごとに、セッションキー発生部316により生成されたセッションキーKs1を復号処理部312によって得られたクラス公開暗号鍵Kpmwを用いて暗号化して、バスBS1に出力するための暗号処理部318と、セッションキーKs1によって暗号化された上で送信されたデータをバスBS1より受けて、復号処理を行なう復号処理部320とを含む。

【0070】データ処理部310は、さらに、配信制御部315から与えられるライセンス鍵Kcおよびアクセス制御情報ACmを、復号処理部320によって得られたメモ리카ードごとに個別公開暗号鍵Kpmcxによって暗号化するための暗号処理部326と、暗号処理部326の出力を、復号処理部320から与えられるセッションキーKs2によってさらに暗号化してバスBS1に出力するための暗号処理部328とを含む。

【0071】配信サーバ10の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0072】図6は、図1に示した携帯電話機100の構成を説明するための概略ブロック図である。

【0073】携帯電話機100は、携帯電話網により無線伝送される信号を受信するアンテナ1100と、アンテナ1100からの信号を受けてベースバンド信号に変換、あるいは携帯電話機100からのデータを変調してアンテナ1100に与える送受信部1102と、携帯電話機100の各部のデータ授受を行なうバスBS2とを含む。

【0074】携帯電話機100は、さらに、携帯電話機100のユーザの音声データを取込み、音声データをAD変換部1106へ出力するマイク1104と、音声データをアナログ信号からデジタル信号に変換するAD変換部1106と、デジタル信号に変換された音声信号を所定の方式に符号化する音声符号化部1108とを含む。

【0075】携帯電話機100は、さらに、他の携帯電話機から受信した音声信号を復号する音声再生部1110と、音声再生部1110からの音声信号をデジタル信号からアナログ信号に変換して音声データを出力するDA変換部1112と、音声データを外部へ出力するスピーカ1114とを含む。

【0076】携帯電話機100は、さらに、外部からの指示を携帯電話機100に与える操作パネル1116と、コントローラ1120等から出力される情報をユーザに視覚情報として与える表示パネル1118と、バスBS2を介して携帯電話機100の動作を制御するコントローラ1120と、メモ리카ード110とバスBS2との間のデータの授受を制御するメモ리카ードインタフェース1200とを含む。

【0077】携帯電話機100は、さらに、クラス公開

暗号鍵Kpplおよびクラス証明書Cpalを公開認証鍵Kpaで復号することでその正当性を認証できる状態に暗号化した認証データ{Kppl/Cpal}Kpaを保持する認証データ保持部1500を含む。ここで、携帯電話機100のクラスyは、y=1であるとする。

【0078】携帯電話機100は、さらに、クラス固有の復号鍵であるKplを保持するKp保持部1502と、バスBS2から受けたデータをKplによって復号し、メモリカード110によって発生されたセッションキーKs2を得る復号処理部1504とを含む。

【0079】携帯電話機100は、さらに、メモリカード110に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード110との間でバスBS2上においてやり取りされるデータを暗号化するためのセッションキーKs3を乱数等により発生するセッションキー発生部1508と、機能証明書Cpb1を保持する機能証明書保持部1507とを含む。ここで、携帯電話機100のクラスiは、i=1であるとする。機能証明書Cpb1は、コンテンツ再生デバイス1550が時間を判定する機能を備えることを示す機能証明書である。

【0080】携帯電話機100は、さらに、暗号化コンテンツデータの再生セッションにおいてメモリカード110からライセンス鍵Kcおよび再生制御情報ACpを受取る際に、機能証明書保持部1507からの機能証明書Cpb1とセッションキー発生部1508により発生されたセッションキーKs3とを復号処理部1504によって得られたセッションキーKs2によって暗号化し、バスBS2に出力する暗号処理部1506と、バスBS2上のデータをセッションキーKs3によって復号して、ライセンス鍵Kcおよび再生制御情報ACpを出力する復号処理部1510と、時間情報を出力する時計1512と、復号処理部1510からライセンス鍵Kcおよび再生制御情報ACpを受け、その受けた再生制御情報ACpに含まれる再生開始日時または再生終了日時と時計1512から得られた時間情報とに基づいて暗号化コンテンツデータ{Dc}Kcの再生が時期的に制限されているか否かを判定し、再生が時期的に制限されていないとき、ライセンス鍵Kcを復号処理部1516へ出力する再生制御部1514とを含む。

【0081】携帯電話機100は、さらに、バスBS2より暗号化コンテンツデータ{Dc}Kcを受けて、再生制御部1514からのライセンス鍵Kcによって暗号化コンテンツデータ{Dc}Kcを復号してコンテンツデータDcを音楽再生部1518へ出力する復号処理部1516と、復号処理部1516からの出力を受けてコンテンツデータを再生するための音楽再生部1518と、音楽再生部1518の出力をデジタル信号からアナログ信号に変換するDA変換部1519と、DA変換

部1519の出力をヘッドホーンなどの外部出力装置(図示省略)へ出力するための端子1530とを含む。

【0082】なお、図6においては、点線で囲んだ領域は暗号化コンテンツデータを復号して音楽データを再生するコンテンツ再生デバイス1550を構成する。

【0083】このように、携帯電話機100は、再生制御情報ACpによって制限される暗号化コンテンツデータの再生期間を判定する機能を備える携帯電話機である。

【0084】図7は、図1に示すデータ配信システムにおける携帯電話機102の構成を説明するための概略ブロック図である。携帯電話機102は、携帯電話機100の時計1512を削除したものであり、その他は携帯電話機100と同じである。なお、携帯電話機102においては、機能証明書保持部1507は、機能証明書Cpb1に代えて機能証明書Cpb2を保持する。機能証明書Cpb2は、コンテンツ再生デバイス1550が時間的な判定機能を有しないことを示す機能証明書である。したがって、携帯電話機102は、再生制御情報ACpによって制限される暗号化コンテンツデータの再生期間を判定できない携帯電話機である。

【0085】図8は、図1に示すデータ配信システムにおける携帯電話機104の構成を説明するための概略ブロック図である。携帯電話機104は、携帯電話機100の機能証明書保持部1507および時計1512を削除したものであり、その他は携帯電話機100と同じである。したがって、携帯電話機104は、機能証明書を備えない携帯電話機である。

【0086】携帯電話機100、102、104の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0087】図9は、図1に示すメモリカード110の構成を説明するための概略ブロック図である。

【0088】すでに説明したように、メモリカードのクラス公開暗号鍵およびクラス秘密復号鍵として、KpmwおよびKmwが設けられ、メモリカードのクラス証明書Cmwが設けられるが、メモリカード110においては、自然数w=3で表わされるものとする。また、メモリカードを識別する自然数xはx=4で表わされるものとする。

【0089】したがって、メモリカード110は、認証データ{Kpm3/Cm3}Kpaを保持する認証データ保持部1400と、メモリカードごとに設定される固有の復号鍵である個別秘密復号鍵Kmc4を保持するKmc保持部1402と、クラス秘密復号鍵Km3を保持するKm保持部1421と、個別秘密復号鍵Kmc4によって復号可能な公開暗号鍵Kpmc4を保持するKpmc保持部1416とを含む。

【0090】このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかに

なるように、配信されたコンテンツデータや暗号化されたライセンス鍵の管理をメモリカード単位で実行することが可能になる。

【0091】メモリカード110は、さらに、メモリインタフェース1200との間で信号を端子1426を介して授受するインタフェース1424と、インタフェース1424との間で信号をやり取りするバスBS3と、バスBS3にインタフェース1424から与えられるデータから、クラス秘密復号鍵Km3をKm保持部1421から受けて、配信サーバ10が配信セッションにおいて生成したセッションキーKs1を接点Paに出力する復号処理部1422と、KPa保持部1414から公開認証鍵KPaを受けて、バスBS3に与えられるデータから公開認証鍵KPaによる復号処理を実行して復号結果と得られたクラス証明書をコントローラ1420に、得られたクラス公開鍵を暗号化処理部1410に出力する復号処理部1408と、切換スイッチ1442によって選択的に与えられる鍵によって、切換スイッチ1446によって選択的に与えられるデータを暗号化してバスBS3に出力する暗号処理部1406とを含む。

【0092】メモリカード110は、さらに、配信、および再生の各セッションにおいてセッションキーKs2を発生するセッションキー発生部1418と、セッションキー発生部1418の出力したセッションキーKs2を復号処理部1408によって得られるクラス公開暗号鍵KPyによって暗号化してバスBS3に送出する暗号処理部1410と、バスBS3よりセッションキーKs2によって暗号化されたデータを受けてセッションキー発生部1418より得たセッションキーKs2によって復号する復号処理部1412とを含む。

【0093】メモリカード110は、さらに、バスBS3上のデータを個別公開暗号鍵Kpmc4と対をなすメモリカード110の個別秘密復号鍵Kmc4によって復号するための復号処理部1404と、暗号化コンテンツデータ{Dc}Kcと、暗号化コンテンツデータ{Dc}Kcを再生するためのライセンス(Kc, ACp, ACm, ライセンスID, コンテンツID)と、付加情報Dc-infと、暗号化コンテンツデータの再生リストと、ライセンスを管理するためのライセンス管理ファイルとをバスBS3より受けて格納するためのメモリ1415とを含む。メモリ1415は、例えば半導体メモリによって構成される。また、メモリ1415は、ライセンス領域1415Aと、データ領域1415Bとから成る。

【0094】ライセンス領域1415Aは、ライセンスを記録するための領域であり、ライセンス(ライセンス鍵Kc、再生制御情報ACp、アクセス制限情報ACm、ライセンスID、コンテンツID)を記録するためにエントリと呼ばれるライセンス専用の記録単位でライセンスを格納する。ライセンスに対してアクセスする場

合には、ライセンスが格納されている、あるいは、ライセンスを記録したいエントリをエントリ番号によって指定する構成になっている。

【0095】データ領域1415Bは、暗号化コンテンツデータ{Dc}Kc、暗号化コンテンツデータの関連情報Dc-inf、ライセンスを管理するために必要な情報を暗号化コンテンツデータごとに記録するライセンス管理ファイル、メモリカードに記録された暗号化コンテンツデータやライセンスにアクセスするための基本的な情報を記録する再生リスト、およびライセンス領域1415Aのエントリを管理するためのエントリ情報を記録するための領域である。そして、データ領域1415Bは、外部から直接アクセスが可能である。ライセンス管理ファイルおよび再生リストの詳細については後述する。

【0096】メモリカード110は、さらに、バスBS3を介して外部との間でデータ授受を行ない、バスBS3との間で再生情報等を受けて、メモリカード110の動作を制御するためのコントローラ1420を含む。

【0097】なお、データ領域1415Bを除く全ての構成は、耐タンパモジュール領域に構成される。

【0098】以下、図1に示すデータ配信システムにおける各セッションの動作について説明する。

【0099】[配信] まず、図1に示すデータ配信システムにおいて、配信サーバ10から携帯電話機100、102、104に装着されたメモリカード110へ暗号化コンテンツデータおよびライセンスを配信する動作について説明する。

【0100】図10および図11は、図1に示すデータ配信システムにおける暗号化コンテンツデータの購入時に発生する携帯電話機100、102、104に装着されたメモリカード110へのライセンスの配信動作(以下、配信セッションともいう)を説明するための第1および第2のフローチャートである。

【0101】図10における処理以前に、携帯電話機100、102、104のユーザは、配信サーバ10に対して電話網を介して接続し、購入を希望するコンテンツに対するコンテンツIDを取得し、さらに、メモリカード110に対するエントリ管理情報を取得してライセンス領域1415A内の空きエントリを確認していることを前提としている。

【0102】図10を参照して、携帯電話機100、102、104のユーザから操作パネル1116を介してコンテンツIDの指定による配信リクエストがなされる(ステップS100)。そして、操作パネル1116を介して暗号化コンテンツデータのライセンスを購入するための購入条件ACを入力するように指示し、購入条件ACが入力される(ステップS102)。つまり、選択した暗号化コンテンツデータを復号するライセンス鍵Kcを購入するために、暗号化コンテンツデータのアクセ

ス制御情報ACm、および再生制御情報ACpを設定して購入条件ACが入力される。

【0103】暗号化コンテンツデータの購入条件ACが入力されると、コントローラ1120は、バスBS2およびメモリカードインタフェース1200を介してメモリカード110へ認証データの出力指示を与える(ステップS104)。メモリカード110のコントローラ1420は、端子1426、インタフェース1424およびバスBS3を介して認証データの送信要求を受信する(ステップS106)。そして、コントローラ1420は、バスBS3を介して認証データ保持部1400から認証データ{Kpm3//Cm3}KPaを読み出し、{Kpm3//Cm3}KPaをバスBS3、インタフェース1424および端子1426を介して出力する(ステップS108)。

【0104】携帯電話機100、102、104のコントローラ1120は、メモリカード110からの認証データ{Kpm3//Cm3}KPaに加えて、コンテンツID、ライセンス購入条件のデータAC、および配信リクエストを配信サーバ10に対して送信する(ステップS110)。

【0105】配信サーバ10では、携帯電話機100、102、104から配信リクエスト、コンテンツID、認証データ{Kpm3//Cm3}KPa、およびライセンス購入条件のデータACを受信し(ステップS112)、復号処理部312においてメモリカード110から出力された認証データを公開認証鍵KPaで復号する(ステップS114)。

【0106】配信制御部315は、復号処理部312における復号処理結果から、正規の機関でその正当性を証明するための暗号化を施した認証データを受信したか否かを判断する認証処理を行なう(ステップS116)。正当な認証データであると判断された場合、配信制御部315は、クラス公開暗号鍵Kpm3およびクラス証明書Cm3を承認し、受理する。そして、次の処理(ステップS118)へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵Kpm3およびクラス証明書Cm3を受理しないで配信セッションを終了する(ステップS164)。

【0107】認証の結果、正当な認証データを持つメモリカードを装着した携帯電話機からのアクセスであることが確認されると、配信サーバ10において、セッションキー発生部316は、配信のためのセッションキーKs1を生成する(ステップS118)。セッションキーKs1は、復号処理部312によって得られたメモリカード110に対応するクラス公開暗号鍵Kpm3によって、暗号処理部318によって暗号化される(ステップS120)。

【0108】配信制御部315は、ライセンスIDを生成し(ステップS122)、ライセンスIDおよび暗号

化されたセッションキーKs1は、ライセンスID/{Ks1}Km3として、バスBS1および通信装置350を介して外部に出力される(ステップS124)。

【0109】携帯電話機100、102、104が、ライセンスID/{Ks1}Km3を受信すると、コントローラ1120は、ライセンスID/{Ks1}Km3をメモリカード110に入力する(ステップS126)。そうすると、メモリカード110においては、端子1426およびインタフェース1424を介して、コントローラ1420は、ライセンスID/{Ks1}Km3を受信する(ステップS128)。そして、コントローラ1420は、バスBS3を介して{Ks1}Km3を復号処理部1422へ与え、復号処理部1422は、Km保持部1421に保持されるメモリカード110に固有なクラス秘密復号鍵Km3によって復号処理することにより、セッションキーKs1を復号し、セッションキーKs1を受信する(ステップS132)。

【0110】コントローラ1420は、配信サーバ10で生成されたセッションキーKs1の受理を確認すると、セッションキー発生部1418に対してメモリカード110において配信動作時に生成されるセッションキーKs2の生成を指示する。そして、セッションキー発生部1418は、セッションキーKs2を生成する(ステップS134)。

【0111】暗号処理部1406は、切換スイッチ1442の接点Paを介して復号処理部1422より与えられるセッションキーKs1によって、切換スイッチ1446の接点を順次切換えることによって与えられるセッションキーKs2、および個別公開暗号鍵Kpmc4を1つのデータ列として暗号化して、{Ks2//Kpmc4}Ks1をバスBS3に出力する。バスBS3に出力された暗号化データ{Ks2//Kpmc4}Ks1は、バスBS3からインタフェース1424および端子1426を介して携帯電話機100、102、104に出力され(ステップS138)、携帯電話機100、102、104から配信サーバ10に送信される(ステップS140)。

【0112】図11を参照して、配信サーバ10は、{Ks2//Kpmc4}Ks1を受信して、復号処理部320においてセッションキーKs1による復号処理を実行し、メモリカード110で生成されたセッションキーKs2、およびメモリカード110の個別公開暗号鍵Kpmc4を受信する(ステップS142)。

【0113】配信制御部315は、ステップS112で取得したコンテンツIDに従ってライセンス鍵Kcを情報データベース304から取得し(ステップS144)、ステップS112で取得したライセンス購入条件のデータACに従って、アクセス制御情報ACmおよび再生制御情報ACpを決定する(ステップS146)。

【0114】配信制御部315は、生成したライセン

ス、すなわち、ライセンスID、コンテンツID、ライセンス鍵Kc、再生制御情報ACp、およびアクセス制御情報ACmを暗号処理部326に与える。暗号処理部326は、復号処理部320によって得られたメモリカード110の個別公開暗号鍵Kpmc4によってライセンスを暗号化して暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4を生成する(ステップS148)。そして、暗号処理部328は、暗号処理部326からの暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4を、復号処理部320からのセッションキーKs2によって暗号化し、暗号化データ{ {ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2を出力する。配信制御部315は、バスBS1および通信装置350を介して暗号化データ{ {ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2を携帯電話機100、102、104へ送信する(ステップS150)。

【0115】携帯電話機100、102、104は、送信された暗号化データ{ {ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2を受信し、バスBS2を介してメモリカード110に入力する(ステップS152)。メモリカード110においては、端子1426およびインタフェース1424を介して、バスBS3に与えられた受信データを復号処理部1412によって復号する。復号処理部1412は、セッションキー発生部1418から与えられたセッションキーKs2を用いてバスBS3の受信データを復号し、バスBS3に出力する(ステップS154)。

【0116】この段階で、バスBS3には、Kmc保持部1402に保持される個別秘密復号鍵Kmc4で復号可能な暗号化ライセンス{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4が出力される(ステップS154)。

【0117】コントローラ1420の指示によって、暗号化ライセンス{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4は、復号処理部1404において、個別秘密復号鍵Kmc4によって復号され、ライセンス(ライセンス鍵Kc、ライセンスID、コンテンツID、アクセス制御情報ACmおよび再生制御情報ACp)が受理される(ステップS156)。

【0118】携帯電話機100、102、104のコントローラ1120は、メモリカード110のメモリ1415から読出したエントリ管理情報に基づいて、配信サーバ10から受信したライセンスを格納するためのエントリ番号を決定し、その決定したエントリ番号をバスBS2およびメモリカードインタフェース1200を介してメモリカード110へ入力する。そして、コントロー

ラ1120は、エントリ管理情報を追加更新する(ステップS158)。

【0119】そうすると、メモリカード110のコントローラ1420は、端子1426およびインタフェース1424を介してエントリ番号を受取り、その受取ったエントリ番号によって指定されるメモリ1415のライセンス領域1415Aに、ステップS156において取得したライセンス(ライセンス鍵Kc、ライセンスID、コンテンツID、アクセス制御情報ACmおよび再生制御情報ACp)を格納する(ステップS160)。ライセンスの書き込みが終了すると、コントローラ1120は、ステップS158においてメモリカード110へ入力したエントリが使用中であるようにエントリ管理情報を更新し、その更新したエントリ管理情報をメモリカード110へ入力する(ステップS162)。メモリカード110のコントローラ1420は、入力されたエントリ管理情報を用いてメモリ1415のデータ領域1415B内にエントリ管理情報を書込む(ステップS163)。そして、ライセンスの配信動作が終了する(ステップS164)。

【0120】ライセンスの配信セッションが終了した後、携帯電話機100、102、104のコントローラ1120は、暗号化コンテンツデータの配信要求を配信サーバ10へ送信し、配信サーバ10は、暗号化コンテンツデータの配信要求を受信する。そして、配信サーバ10の配信制御部315は、情報データベース304より、暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infを取得して、これらのデータをバスBS1および通信装置350を介して出力する。

【0121】携帯電話機100、102、104は、{Dc}Kc//Dc-infを受信して、暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infを受理する。そうすると、コントローラ1120は、暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infを1つのコンテンツファイルとしてバスBS2およびメモリカードインタフェース1200を介してメモリカード110に入力する。また、コントローラ1120は、メモリカード110に格納されたライセンスのエントリ番号と、平文のライセンスIDおよびコンテンツIDを含む暗号化コンテンツデータ{Dc}Kcと付加情報Dc-infに対するライセンス管理ファイルを生成し、バスBS2およびメモリカードインタフェース1200を介してメモリカード110に入力する。さらに、コントローラ1120は、メモリカード110のメモリ1415に記録されている再生リストに、受理したコンテンツの情報として、記録したコンテンツファイル及びライセンス管理ファイルの名称や付加情報Dc-infから抽出した暗号化コンテンツデータに関する情報(曲名、アーティスト名)等を追記し、全体の処理が終了する。

【0122】このようにして、携帯電話機100、102、104に装着されたメモリカード110が正規の認証データを保持する機器であること、同時に、クラス証明書Cm3とともに暗号化して送信できた公開暗号鍵Kp3が有効であることを確認した上でコンテンツデータを配信することができ、不正なメモリカードへのコンテンツデータの配信を禁止することができる。

【0123】さらに、配信サーバおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データ10を相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【0124】図12を参照して、メモリカード110のメモリ1415におけるライセンス領域1415Aとデータ領域1415Bとについて説明する。データ領域1415Bには、再生リストファイル160と、エントリ管理情報165と、コンテンツファイル1611~161nと、ライセンス管理ファイル1621~162nとが記録されている。コンテンツファイル1611~161nは、受信した暗号化コンテンツデータ{Dc}Kcと付加情報Dc-infとを1つのファイルとして記録する。また、ライセンス管理ファイル1621~162nは、それぞれ、コンテンツファイル1611~161nに対応して記録されている。

【0125】メモリカード110は、配信サーバ10から暗号化コンテンツデータおよびライセンスを受信したとき、暗号化コンテンツデータおよびライセンスをメモリ1415に記録する。

【0126】したがって、配信サーバ10からメモリカード110へ送信された暗号化コンテンツデータのライセンスは、メモリ1415のライセンス領域1415Aのエントリ番号によって指定された領域に記録され、メモリ1415のデータ領域1415Bに記録された再生リストファイル160のライセンス管理ファイルを読出せば、エントリ番号を取得でき、その取得したエントリ番号によって対応するライセンスをライセンス領域1415Aから読出すことができる。

【0127】【再生】上述したように、携帯電話機100、102、104に装着されたメモリカード110は、配信サーバ10から暗号化コンテンツデータおよびライセンスを受信できる。そこで、次に、メモリカードが受信した暗号化コンテンツデータの再生について説明する。

【0128】図13は、メモリカード110が受信したコンテンツデータの携帯電話機100、102、104における再生動作を説明するためのフローチャートである。なお、図13における処理以前に、携帯電話機100、102、104のユーザは、メモリカード110の

データ領域1415Bに記録されている再生リストに従って、再生するコンテンツ（楽曲）を決定し、コンテンツファイルを特定し、ライセンス管理ファイルを取得していることを前提として説明する。

【0129】図13を参照して、再生動作の開始とともに、携帯電話機100、102、104のユーザから操作パネル1116を介して再生リクエストが携帯電話機100、102、104にインプットされる（ステップS10）。そうすると、携帯電話機100、102、104とメモリカード110との間で初期化処理が行なわれる（ステップS20）。この初期化処理の詳細については後述する。初期化処理が終了すると、携帯電話機100、102、104のコントローラ1120は、初期化処理においてエラーが発生したか否かを判定し（ステップS30）、エラーが発生した場合は、暗号化コンテンツデータの再生動作は終了する（ステップS70）。

【0130】ステップS30において、コントローラ1120が初期化処理においてエラーが発生していないと判定したとき、再生許諾処理が行なわれる（ステップS40）。この再生許諾処理の詳細についても後述する。再生許諾処理が終了すると、携帯電話機100、102、104のコントローラ1120は、再生許諾処理においてエラーが発生したか否かを判定し（ステップS50）、エラーが発生したとき再生許諾処理（ステップS40）を繰返し行なう。ステップS50において、コントローラ1120が再生許諾処理においてエラーが発生しなかったと判定したとき、再生処理が行なわれる（ステップS60）。その後、ステップS40、S50、S60が繰返されて暗号化コンテンツデータの再生が行なわれる。したがって、再生動作において、一度、初期化処理を行なえば、2回目以降、初期化処理を行なうことなく、暗号化コンテンツデータを再生することができる。

【0131】図14は、図13に示す初期化処理の動作を詳細に説明するためのフローチャートである。図14を参照して、図13に示すステップS10において再生リクエストがされると、コントローラ1120は、バスBS2を介して認証データの出力要求をコンテンツ再生デバイス1550に行ない（ステップS200）、コンテンツ再生デバイス1550は認証データの出力要求を受信する（ステップS202）。そして、認証データ保持部1500は、認証データ{Kp1/Cp1}KPaを出力し（ステップS204）、コントローラ1120は、メモリカードインタフェース1200を介してメモリカード110へ認証データ{Kp1/Cp1}KPaを入力する（ステップS206）。

【0132】そうすると、メモリカード110は、認証データ{Kp1/Cp1}KPaを受理し（ステップS208）、復号処理部1408は、受理した認証データ{Kp1/Cp1}KPaを、KPa保持



部1414に保持された公開認証鍵KPaによって復号し(ステップS210)、コントローラ1420は復号処理部1408における復号処理結果から、認証処理を行なう。すなわち、認証データ{Kp1//Cpa1}KPaが正規の認証データであるか否かを判断する認証処理を行なう(ステップS212)。復号できなかった場合、ステップS222へ移行し、初期化処理は終了する。認証データが復号できた場合、コントローラ1420は、セッションキー発生部1418を制御し、セッションキー発生部1418は、再生セッション用のセッションキーKs2を発生させる(ステップS214)。そして、暗号処理部1410は、セッションキー発生部1418からのセッションキーKs2を、復号処理部1408で復号された公開暗号鍵Kp1によって暗号化した暗号化データ{Ks2}Kp1をバスBS3へ出力する。そうすると、コントローラ1420は、インタフェース1424および端子1426を介してメモリカードインタフェース1200へ暗号化データ{Ks2}Kp1を出力する(ステップS216)。携帯電話機100、102、104のコントローラ1120は、メモリカードインタフェース1200を介して暗号化データ{Ks2}Kp1を取得する。そして、コントローラ1120は、暗号化データ{Ks2}Kp1をバスBS2を介してコンテンツ再生デバイス1550の復号処理部1504へ与え(ステップS218)、復号処理部1504は、Kp保持部1502から出力された、公開暗号鍵Kp1と対になっている秘密復号鍵Kp1によって暗号化データ{Ks2}Kp1を復号し、セッションキーKs2を受理する(ステップS220)。そして、初期化処理が終了する(ステップS222)。

【0133】図15は、図13に示す再生許諾処理(ステップS40)の動作を詳細に説明するためのフローチャートである。なお、図15は、携帯電話機100、102とメモリカード110との間における再生許諾処理の動作を示したフローチャートである。図15を参照して、図13に示すステップS30においてエラーが発生しなかったと判定されると、携帯電話機100、102のコントローラ1120は、セッションキーKs3を発生するようにセッションキー発生部1508を制御し(ステップS300)、セッションキー発生部1508は、再生セッション用のセッションキーKs3を発生させ、セッションキーKs3を暗号処理部1506へ出力する(ステップS304)。暗号処理部1506は、セッションキー発生部1508からのセッションキーKs3と機能証明書保持部1507からの機能証明書Cpb1とを復号処理部1504からのセッションキーKs2によって暗号化して{Ks3//Cpb1}Ks2を出力し(ステップS306)、コントローラ1120は、バスBS2およびメモリカードインタフェース1200を介して{Ks3//Cpb1}Ks2をメモリカード

110へ出力する(ステップS308)。

【0134】そうすると、メモリカード110の復号処理部1412は、端子1426、インタフェース1424、およびバスBS3を介して{Ks3//Cpb1}Ks2を受ける。復号処理部1412は、セッションキー発生部1418によって発生されたセッションキーKs2によって{Ks3//Cpb1}Ks2を復号して、携帯電話機100、102で発生されたセッションキーKs3と機能証明書Cpb1とを受理する(ステップS310)。

【0135】携帯電話機100、102のコントローラ1120は、メモリカード110から事前に取得した再生リクエスト曲のライセンス管理ファイルからライセンスの格納されているエントリ番号を取得し、取得したエントリ番号とライセンス出力要求とをメモリカードインタフェース1200を介してメモリカード110へ入力する(ステップS312)。

【0136】メモリカード110のコントローラ1420は、エントリ番号とライセンス出力要求とを受理し、エントリ番号によって指定された領域に格納されたライセンスを取得する(ステップS314)。そして、コントローラ1420は、取得したライセンスから再生制御情報ACpを讀出して再生制御情報ACp内の再生制限フラグを確認し、ステップS314において受理した機能証明書Cpb1によって再生制限フラグがアクティブ「1」となっている再生制限に従って再生を行なう機能を備えているか否か、すなわち、機能証明書を出力したコンテンツ再生デバイス1550が再生制御情報ACpに対応しているか否かを判定する(ステップS316)。

【0137】メモリカード110が携帯電話機100から機能証明書を受理したとき、その機能証明書は、携帯電話機100のコンテンツ再生デバイス1550が時間を判定する機能を備えていることを示す機能証明書Cpb1であるので、コントローラ1420は、再生制御情報ACpの時間に関する制限があることを示すフラグFG4、FG5のいずれかがアクティブ「1」の場合には対応できると判断する。フラグFG4、FG5が共にネガティブ「0」の場合には、時間に関する制限を受けないため、コントローラ1420は、対応できると判断する。

【0138】一方、メモリカード110が携帯電話機102から機能証明書を受理したとき、その機能証明書は、携帯電話機102のコンテンツ再生デバイス1550が時間を判定する機能を備えないことを示す機能証明書Cpb2であるので、コントローラ1420は、再生制御情報ACpの時間に関する制限があることを示すフラグFG4、FG5のいずれかがアクティブ「1」の場合には対応できないと判断する。フラグFG4、FG5が共にネガティブ「0」の場合には、時間に関する制限

を受けないため、コントローラ1420は、対応できると判断する。また、コントローラ1420は、再生制御情報ACpにおいて再生開始日時および再生終了日時の指定がなされていないとき、機能証明書Cpb2が再生制御情報ACpに対応していると判定する。

【0139】また、フラグFG3については、携帯電話機100または携帯電話機102のコンテンツ再生デバイス1550が地域コードを保持し、その地域コードに対応した地域で再生を許可されたコンテンツデータのみを再生する場合、それぞれの機能証明書には、地域コード対応が記載されていることとなり、フラグFG3がアクティブ「1」の場合には、機能証明書によって地域コード対応とされた場合に対応可能と判断する。逆に、フラグFG3がネガティブ「0」の場合には、地域コードによる制限を受けない全地域において再生が可能なコンテンツであり、機能証明書によらないで全ての機器において対応可能と判断する。他のフラグFG1、FG2についても同様である。

【0140】このようにしてステップS316では、再生制限フラグを構成する全てのフラグFG1～FG5に対して対応可能であると判断されたとき、コントローラ1420は、再生制御情報ACpに記載されていると判断し、いずれか一つでも対応できない場合には対応不可と判断する。

【0141】ステップS316において、コントローラ1420は、機能証明書Cpbiによってコンテンツ再生デバイス1550が再生制御情報ACpに対応していないと判定したとき、再生許諾処理は終了する（ステップS330）。ステップS316において、コントローラ1420は、機能証明書Cpbiが再生制御情報ACpに対応していると判定したとき、ライセンスに含まれるアクセス制限情報ACmを確認する（ステップS318）。

【0142】ステップS318においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報ACmを確認することにより、具体的には、再生回数を確認することにより、既に再生不可の状態である場合には再生動作を終了し、アクセス制限情報の再生回数に制限がある場合にはアクセス制限情報ACmの再生回数を変更した（ステップS320）後に次のステップに進む（ステップS322）。一方、アクセス制限情報ACmの再生回数によって再生が制限されていない場合においては、ステップS318はスキップされ、アクセス制限情報ACmの再生回数は変更されことなく処理が次のステップ（ステップS322）に進行される。

【0143】ステップS318において、当該再生動作において再生が可能であると判断された場合には、メモリ1415のライセンス領域1415Aに記録された再生リクエスト曲のライセンス鍵Kcおよび再生制御情報ACpがバスBS3上に出力される（ステップS32

2）。

【0144】得られたライセンス鍵Kcと再生制御情報ACpは、バスBS3を介して暗号処理部1406に送られる。暗号処理部1406は、切換スイッチ1442の接点Pbを介して復号処理部1412より受けたセッションキーKs3によってバスBS3を介して受けたライセンス鍵Kcと再生制御情報ACpとを暗号化し、(Kc//ACp)Ks3をバスBS3に出力する。

【0145】バスBS3に出力された暗号化データ(Kc//ACp)Ks3は、インタフェース1424、端子1426、およびメモ리카ードインタフェース1200を介して携帯電話機100、102に出力される（ステップS322）。

【0146】携帯電話機100、102のコントローラ1120は、メモ리카ードインタフェース1200およびバスBS2を介して暗号化データ(Kc//ACp)Ks3を受取り、その受取った暗号化データ(Kc//ACp)Ks3をバスBS2を介してコンテンツ再生デバイス1550の復号処理部1510に与える（ステップS324）。そして、復号処理部1510は、バスBS2を介して与えられた暗号化データ(Kc//ACp)Ks3を、セッションキー発生部1508からのセッションキーKs3によって復号処理を行ない、ライセンス鍵Kcおよび再生制御情報ACpを再生制御部1514へ出力する。これによってライセンス鍵Kcおよび再生制御情報ACpが受理される（ステップS326）。

【0147】再生制御部1514は、再生制御情報ACpに基づいて暗号化コンテンツデータ(Dc)Kcの再生が可能か否かを判定する（ステップS328）。具体的には、携帯電話機100の場合、コンテンツ再生デバイスはフラグFG3～FG5に対応しているとする、再生制御部1514は、再生制限フラグのフラグFG3～FG5のいずれがアクティブ「1」であるかを確認する。そして、フラグFG3がアクティブ「1」である場合、再生制御部1514は、内部に保持した地域コードを、再生制御情報ACpの領域21に記載されている地域コードと比較し、不一致であるとき再生許諾動作を終了する。また、フラグFG4またはフラグFG5がアクティブ「1」である場合、再生制御部1514は、時計1512から時間情報を取得し、その取得した時間情報と再生制御情報ACpに含まれる再生開始日時または再生終了日時とに基づいて、暗号化コンテンツデータ(Dc)Kcの再生が再生開始日時または再生終了日時によって制限されているかを判定し、暗号化コンテンツデータ(Dc)Kcの再生が再生開始日時または再生終了日時によって制限されているとき、暗号化コンテンツデータ(Dc)Kcの再生許諾動作が終了する（ステップS330）。再生制御部1514は、暗号化コンテンツデータ(Dc)Kcの再生が再生制御情報ACpによ

って制限されていないと判定したとき、ライセンス鍵Kcを復号処理部1516へ出力し、後述する暗号化コンテンツデータ{Dc}Kcの再生処理が行なわれる。

【0148】一方、携帯電話機102の場合、コンテンツ再生デバイスは、フラグFG3にのみ対応し、フラグFG4、FG5には対応しない。しかし、ステップS316の処理によってフラグFG4、FG5は必ずネガティブ「0」である。再生制御部1514は、再生制限フラグのフラグがアクティブ「1」であるかを確認する。そして、フラグFG3がアクティブ「1」である場合、再生制御部1514は、内部に保持した地域コードを、再生制御情報ACpの領域21に記載されている地域コードと比較して不一致のとき再生許諾動作が終了する（ステップS330）。再生制御部1514は、保持した地域コードが再生制御情報ACpの領域21に記載された地域コードと一致したとき、ライセンス鍵Kcを復号処理部1516へ出力し、後述する暗号化コンテンツデータ{Dc}Kcの再生処理が行なわれる。

【0149】そして、再生許諾処理が終了する（ステップS330）。このように、再生許諾処理においては、携帯電話機100、102からメモ리카ード110へ送信された機能証明書Cpb iが暗号化コンテンツデータ{Dc}Kcの再生制御情報ACpに対応しているか否かがメモ리카ード110において判定され（ステップS316参照）、機能証明書Cpb iが再生制御情報ACpに対応していないとき再生許諾処理が終了する。したがって、再生制御情報ACpによって制限される機能に対応する機能を備えない携帯電話機にメモ리카ードが装着されたとき、暗号化コンテンツデータを復号および再生するためのライセンスはメモ리카ード110から携帯電話機100、102へ出力されず、暗号化コンテンツデータ{Dc}Kcの再生を制限することができる。

【0150】再生許諾処理のステップS328において、再生制御部1514は、暗号化コンテンツデータ{Dc}Kcの再生が可能であると判定したとき、その判定結果をバスBS2を介してコントローラ1120へ出力し、ライセンス鍵Kcを復号処理部1516へ出力する。そして、コントローラ1120は、メモ리카ードインタフェース1200を介してメモ리카ード110に暗号化コンテンツデータ{Dc}Kcを要求する。そうすると、メモ리카ード110のコントローラ1420は、メモリ1415から暗号化コンテンツデータ{Dc}Kcを取得し、バスBS3、インタフェース1424、および端子1426を介してメモ리카ードインタフェース1200へ暗号化コンテンツデータ{Dc}Kcを出力する。

【0151】携帯電話機110、102のコントローラ1120は、メモ리카ードインタフェース1200を介して暗号化コンテンツデータ{Dc}Kcを取得し、バスBS2を介して暗号化コンテンツデータ{Dc}Kc

をコンテンツ再生デバイス1550へ与える。

【0152】そして、コンテンツ再生デバイス1550の復号処理部1516は、暗号化コンテンツデータ{Dc}Kcを再生制御部1514から出力されたライセンス鍵Kcによって復号してコンテンツデータDcを取得する。

【0153】そして、復号されたコンテンツデータDcは音楽再生部1518へ出力され、音楽再生部1518は、コンテンツデータDcを再生し、DA変換部1519はディジタル信号をアナログ信号に変換して端子1530へ出力する。そして、音楽データは端子1530から外部出力装置を介してヘッドホン130へ出力されて再生される。これによって再生動作が終了する。

【0154】また、機能証明書を備えない携帯電話機104における再生許諾処理は、図15のステップS306、S308、S310を図16に示すステップS306a、S308a、S310a、S311に代えたフローチャートに従って行なわれる。図15に示すステップS304の後、携帯電話機104の暗号処理部1506は、セッションキー発生部1508からのセッションキーKs3を、復号処理部1504からのセッションキーKs2によって暗号化して暗号化データ{Ks3}Ks2をバスBS2へ出力する（ステップS306a）。そして、コントローラ1120は、暗号化データ{Ks3}Ks2をバスBS2を介して受取り、メモ리카ードインタフェース1200を介してメモ리카ード110へ出力する（ステップS308a）。そうすると、メモ리카ード110のコントローラ1420は、端子1426、インタフェース1424、およびバスBS3を介して暗号化データ{Ks3}Ks2を受取り、その受取った暗号化データ{Ks3}Ks2をバスBS3を介して復号処理部1412に与える。復号処理部1412は、暗号化データ{Ks3}Ks2を、セッションキー発生部1418からのセッションキーKs2によって復号する（ステップS310a）。

【0155】そうすると、コントローラ1420は、ステップS310aにおいて機能証明書が入力されてこないでコンテンツ再生デバイスに要求される標準の機能が備えられているものとして、デフォルト値を携帯電話機104に内蔵されたコンテンツ再生デバイス1550の機能証明書Cpb iとして受理する（ステップS311）。ステップS311の後、図15に示すステップS312～S330が実行されて携帯電話機104における再生許諾処理が終了する。ステップS311において受理されたデフォルト値は、図3に示すフラグFG1、FG2による再生制限に対応可能であり、暗号化コンテンツデータ{Dc}Kcの再生制御情報ACpに再生速度および編集可否に関する制限情報が設定されている場合は、図15に示すステップS316において機能証明書が再生制御情報ACpに対応していると判定される。

【0156】このように、機能証明書を備えない携帯電話機にメモ리카ードが装着された場合でも、デフォルト値を機能証明書として用いることによって図15および図16に示すフローチャートに従って暗号化コンテンツデータの再生許諾処理を実行でき、機能証明書を備えない携帯電話機においても、暗号化コンテンツデータの再生を行なうことができる。

【0157】実施の形態1によれば、携帯電話機は、機能証明書を備え、メモ리카ードは携帯電話機から送信された機能証明書が再生制御情報に対応している場合に暗号化コンテンツデータを復号および再生するライセンス鍵を携帯電話機へ出力するので、再生制御情報に制限情報を設定するだけで暗号化コンテンツデータの再生を容易に制限できる。

【0158】【実施の形態2】図17を参照して、実施の形態2による携帯電話機100Aは、携帯電話機100の機能証明書保持部1507を機能証明書保持部1507Aに代えたものであり、その他は携帯電話機100と同じである。機能証明書保持部1507Aは、機能証明書Cpb1をコンテンツ再生デバイス1550に固有な公開暗号鍵Kpp1によって暗号化した暗号化データ(Cpb1)Kpp1の形式で機能証明書Cpb1を保持する。

【0159】図18を参照して、実施の形態2による携帯電話機102Aは、携帯電話機102の機能証明書保持部1507を機能証明書保持部1507Aに代えたものであり、その他は携帯電話機102と同じである。機能証明書保持部1507Aは、機能証明書Cpb2をコンテンツ再生デバイス1550に固有な公開暗号鍵Kpp1によって暗号化した暗号化データ(Cpb1)Kpp1の形式で機能証明書Cpb2を保持する。

【0160】このように、実施の形態2においては、携帯電話機100A、102Aは、機能証明書Cpbiをコンテンツ再生デバイス1550に固有な公開暗号鍵Kpp1によって署名した形式で保持する。そして、メモ리카ードは、暗号化データ(Cpb1)Kpp1を公開暗号鍵Kpp1によって復号し、機能証明書Cpbiを受理したか否かを判定することによって機能証明書Cpbiを正規なコンテンツ再生デバイスから受理したことを確認できる。

【0161】図19を参照して、実施の形態2によるメモ리카ード110Aは、メモ리카ード110に復号処理部1409を追加したものであり、その他は、メモ리카ード110と同じである。復号処理部1409は、再生許諾処理において、暗号化データ(Cpb1)Kpp1を、復号処理部1408によって復号された公開暗号鍵Kpp1によって復号して機能証明書Cpbiを取得する。この場合、復号処理部1408は、認証データ(Kpp1//Cpal)を公開認証鍵Kpaによって復号して得られた公開暗号鍵Kpp1を暗号処理部1410

および復号処理部1409へ出力する。

【0162】暗号化コンテンツデータを再生する際に、携帯電話機100A、102A、104とメモ리카ード110Aとの間で行なわれる初期化処理は、図14に示すフローチャートに従って行なわれる。また、再生許諾処理は、図20に示すフローチャートに従って行なわれる。図20に示すフローチャートは、図15に示すフローチャートにおいてステップS306、S308、S310をステップS306b、S308b、S310b、S310c、S310dに代えたものであり、その他は図15に示すフローチャートと同じである。

【0163】ステップS304の後、携帯電話機100A、102A、104の暗号処理部1506は、機能証明書保持部1507Aからの機能証明書(Cpbi)Kpp1とセッションキー発生部1508からのセッションキーKs3とを、復号処理部1504からのセッションキーKs2によって暗号化し、暗号化データ{(Cpbi)Kpp1//Ks3}Ks2をバスBS2へ出力する(ステップS306b)。コントローラ1120は、バスBS2上の暗号化データ{(Cpbi)Kpp1//Ks3}Ks2をメモ리카ードインタフェース1200を介してメモ리카ード110Aへ入力する(ステップS308b)。

【0164】そうすると、メモ리카ード110Aにおいては、コントローラ1420は、端子1426、インタフェース1424およびバスBS3を介して暗号化データ{(Cpbi)Kpp1//Ks3}Ks2を受取り、その受取った暗号化データ{(Cpbi)Kpp1//Ks3}Ks2をバスBS3を介して復号処理部1412に与える。そして、復号処理部1412は、暗号化データ{(Cpbi)Kpp1//Ks3}Ks2を、セッションキー発生部1418からのセッションキーKs2によって復号し、暗号化データ(Cpbi)Kpp1およびセッションキーKs3を受理する(ステップS310b)。復号処理部1412は、復号して得られた暗号化データ(Cpbi)Kpp1を復号処理部1409へ出力し、セッションキーKs3をスイッチ1442の接点Pbへ出力する。

【0165】そして、復号処理部1409は、暗号化データ(Cpbi)Kpp1を、復号処理部1408からの公開暗号鍵Kpp1によって復号し、機能証明書CpbiをバスBS3へ出力する(ステップS310c)。コントローラ1420は、機能証明書Cpbiを受理したか否かを判定し(ステップS310d)、機能証明書Cpbiを受理しないとき、再生許諾処理は終了する(ステップS330)。ステップS310dにおいて、コントローラ1420が機能証明書Cpbiを受理したと判定したときステップS312~S330が行なわれて再生許諾処理が終了する。

【0166】メモ리카ード110Aが携帯電話機104

に装着されたとき、図20に示すフローチャートのステップS306b、S308b、S310b、S310c、S310dを図16に示すステップS306a、S308a、S310a、S311に代えたフローチャートに従って携帯電話機104における再生許諾処理が行なわれる。

【0167】その他は、実施の形態1と同じである。実施の形態2によれば、携帯電話機は、機能証明書をコンテンツ再生デバイスに固有な公開暗号鍵によって署名した形式で保持するので、公開暗号鍵を保持するメモ리카ードのみが機能証明書を受理することができ、不正なメモ리카ードが機能証明書を受理するのを防止できる。

【0168】【実施の形態3】図21を参照して、実施の形態3による携帯電話機100Bは、携帯電話機100Aの機能証明書保持部1507Aを機能証明書保持部1507Bに代えたものであり、その他は携帯電話機100Aと同じである。機能証明書保持部1507Bは、機能証明書{Cpb1}Kpp1をバスBS2へ直接出力する。

【0169】図22を参照して、実施の形態3による携帯電話機102Bは、携帯電話機102Aの機能証明書保持部1507Aを機能証明書保持部1507Bに代えたものであり、その他は携帯電話機102Aと同じである。機能証明書保持部1507Bは、機能証明書{Cpb2}Kpp1をバスBS2へ直接出力する。

【0170】図23を参照して、実施の形態3によるメモ리카ード110Bは、実施の形態2によるメモ리카ード110Aと同じ構成要素から成るが、復号処理部1412は、セッションキーKs2によって暗号化データを復号した結果を復号処理部1409へ出力しない点、および復号処理部1409は、バスBS3との間でデータをやり取りする点がメモ리카ード110Aと異なる。

【0171】実施の形態3によるメモ리카ード110Bは、携帯電話機100B、102Bから認証データ{Kpp1//Cpa1}Kpaと機能証明書{Cpb1}Kpp1とを初期化処理において受信することに対応したメモ리카ードである。

【0172】図24を参照して、実施の形態3による暗号化コンテンツデータの再生処理における初期化処理について説明する。図24に示すフローチャートは、図14に示すフローチャートのステップS204、S206、S208をステップS204a、S206a、S208aに代え、ステップS212とステップS214との間にステップS213a、S213bを挿入したものであり、その他は図14に示すフローチャートと同じである。ステップS202の後、携帯電話機100B、102Bのコントローラ1120は、コンテンツ再生デバイス1550の認証データ保持部1500および機能証明書保持部1507Bへそれぞれ認証データ{Kpp1//Cpa1}Kpaおよび機能証明書{Cpb1}K

Pp1を出力するように要求し、認証データ保持部1500は、認証データ{Kpp1//Cpa1}KpaをバスBS2へ出力し、機能証明書保持部1507Bは、機能証明書{Cpb1}Kpp1をバスBS2へ出力する(ステップS204a)。そして、コントローラ1120は、バスBS2およびメモ리카ードインタフェース1200を介して{Kpp1//Cpa1}Kpa//{Cpb1}Kpp1をメモ리카ード110Bへ出力する(ステップS206a)。

【0173】そうすると、メモ리카ード110Bのコントローラ1420は、端子1426、インタフェース1424およびバスBS3を介して暗号化データ{Kpp1//Cpa1}Kpa//{Cpb1}Kpp1を受取る(ステップS208a)。その後、上述したステップS210、S212が実行される。そして、コントローラ1420は、暗号化データ{Cpb1}Kpp1を復号処理部1409に与え、復号処理部1409は、暗号化データ{Cpb1}Kpp1を復号処理部1408からの公開暗号鍵Kpp1によって復号し(ステップS213a)、機能証明書Cpb1をバスBS3へ出力する。コントローラ1420は、機能証明書Cpb1を受理したか否かを判定し(ステップS213b)、機能証明書Cpb1を受理しなかったとき初期化処理が終了する(ステップS222)。ステップS213bにおいてコントローラ1420が機能証明書Cpb1を受理したと判定したとき上述したステップS214~S220が実行されて初期化処理が終了する。

【0174】図25を参照して、メモ리카ード110Bが携帯電話機104に装着された場合の初期化処理について説明する。図25に示すフローチャートは図14に示すフローチャートのステップS212とステップS214との間にステップS213、S213bを挿入したものであり、その他は図14に示すフローチャートと同じである。

【0175】ステップS212において、メモ리카ード110Bのコントローラ1420は、公開暗号鍵Kpp1を受理したと判定すると、デフォルト値を携帯電話機104のコンテンツ再生デバイス1550の機能証明書Cpb1として受理する(ステップS213)。そして、コントローラ1420は、機能証明書Cpb1を受理したか否かを判定し(ステップS213b)、機能証明書Cpb1を受理しなかったとき初期化処理が終了する(ステップS222)。ステップS213bにおいてコントローラ1420が機能証明書Cpb1を受理したと判定したとき上述したステップS214~S220が実行されて初期化処理が終了する。ステップS213においてデフォルト値を機能証明書Cpb1として受理しているのでコントローラ1420は、ステップS213bにおいて機能証明書Cpb1を受理したと判定する。

【0176】このように、メモ리카ードが機能証明書を

10

20

30

40

50

備えない携帯電話機に装着された場合でも、初期化処理が実行されて暗号化コンテンツデータの再生が行なわれる。

【0177】図26を参照して、実施の形態3における再生許諾処理の動作について説明する。図26に示すフローチャートは、図15に示すフローチャートのステップS306、S308、S310をステップS306a、S308a、S310aに代えたものであり、その他は図15に示すフローチャートと同じである。ステップS304の後、携帯電話機100B、102B、104の暗号処理部1506は、セッションキー発生部1508からのセッションキーKs3を、復号処理部1504からのセッションキーKs2によって暗号化して暗号化データ{Ks3}Ks2をバスBS2へ出力する(ステップS306a)。そして、コントローラ1120は、暗号化データ{Ks3}Ks2をバスBS2を介して受渡し、メモリカードインタフェース1200を介してメモリカード110Bへ出力する(ステップS308a)。そうすると、メモリカード110Bのコントローラ1420は、端子1426、インタフェース1424、およびバスBS3を介して暗号化データ{Ks3}Ks2を受取り、その受取った暗号化データ{Ks3}Ks2をバスBS3を介して復号処理部1412に与える。復号処理部1412は、暗号化データ{Ks3}Ks2を、セッションキー発生部1418からのセッションキーKs2によって復号してセッションキーKs3を受渡しする(ステップS310a)。その後、ステップ312〜S328が実行されて再生許諾処理が終了する(ステップS330)。

【0178】その他は、実施の形態1と同じである。実施の形態3によれば、暗号化コンテンツデータの再生処理における初期化処理において認証データと機能証明書とが携帯電話機からメモリカードへ送信されるので、携帯電話機の機能を1回確認すれば、以後、携帯電話機の機能を確認しなくても暗号化コンテンツデータを再生できる。

【0179】上記においては、フラグFG1、FG2に関しては機能証明に記載されないものとして説明したが、フラグFG1は再生速度変更禁止を示すことから、再生速度を変更することができないコンテンツ再生デバイスや再生速度を変更することができるがフラグFG1がアクティブ「1」の場合に変更を行なわないように制御できるコンテンツ再生デバイスに対する機能証明書は対応可能であるとして記載され、コンテンツ再生デバイスはフラグFG1がアクティブ「1」であるときには必ず指定の速度で再生する。

【0180】また、フラグFG2は編集可否であることから、フラグFG2がアクティブ「1」の場合には特殊再生に用いることが禁止されるため、フラグFG2に従って特殊再生に帰依しないように再生を行なうことが可

能なコンテンツ再生デバイスに対する機能証明書は対応可能であるとして記載され、コンテンツ再生デバイスは、フラグFG2がアクティブ「1」のコンテンツを特殊再生時には再生しないように制御することで機能証明に追加することも可能である。

【0181】さらに、コンテンツ再生デバイスの標準機能を予め定めた上で、未対応の機能がある場合には、機能証明書に対して機能しない旨を機能証明書に記載することも可能である。

【0182】また、さらに、機能証明書に対して再生制限フラグを構成する各フラグと一意に対応するフラグによって構成される対応機能フラグを設けて機能を記載することもでき、この場合にはステップS316における判断は、再生制限フラグと再生機能対応フラグとの位置を確認すればよい。

【0183】実施の形態1〜実施の形態3においては、携帯電話機に備えられたメモリカードに対してコンテンツデータとして音楽データをダウンロードして記録し、携帯電話機に備えられたコンテンツ再生デバイスによってメモリカードに記録された音楽データを再生するように説明したが、本発明は、これに限定されるものではない。

【0184】本発明は、音楽データのみならず、画像データ、動画データ、テキストデータ、朗読データ、音源データ、およびゲーム等のアプリケーションプログラム等に対応可能であり、著作権者あるいはデータの権利者の権利を守る必要があるデータ全般に適用可能である。

【0185】また、携帯電話網を介してライセンスをダウンロードするように説明したが、データの供給源を規定するものではなく、インターネット等のデジタル通信網に対しても適用可能である。さらに、パーソナルコンピュータなどの機器でメモリカードに、直接、書込むことも可能である。

【0186】さらに、ライセンスを記録する記録装置としてメモリカードを例に挙げて説明したが、メモリカードに限定するものではなく、ハードディスクなどの入出力の制御を行なえる記録装置であれば、いかなる媒体であってもかまわない。

【0187】また、さらに、ライセンスと暗号化コンテンツデータは、必ずしも同一の記録装置上に記録される必要はなく、暗号化コンテンツデータは従来の記録装置に記録されていてもかまわない。

【0188】また、さらに、コンテンツ再生デバイスは、携帯電話機に備えられているように説明したが、携帯電話機は必ずしも必要ではない。そして、配信サーバに接続してダウンロードする機能を同一端末が持つ必要はなく、記録装置(メモリカード)は、ライセンスを記録するためのダウンロード端末と、記録装置(メモリカード)から暗号化コンテンツデータとライセンスとを取得して再生するコンテンツ再生デバイスを備える再生端

末とから構成されていてもよい。

【0189】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【0190】

【発明の効果】本発明によれば、携帯電話機は、機能証明書を書き込み、メモリカードは携帯電話機から送信された機能証明書が再生制御情報に対応している場合に暗号化コンテンツデータを復号および再生するライセンス鍵を携帯電話機へ出力するので、再生制御情報に制限情報を設定するだけで暗号化コンテンツデータの再生を容易に制限できる。

【図面の簡単な説明】

【図1】 データ配信システムを概念的に説明する概略図である。

【図2】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図3】 図2に示す再生制御情報のフォーマットを示す図である。

【図4】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図5】 図1に示すデータ配信システムにおける配信サーバの構成を示す概略ブロック図である。

【図6】 実施の形態1による携帯電話機の構成を示す概略ブロック図である。

【図7】 実施の形態1による他の携帯電話機の構成を示す概略ブロック図である。

【図8】 実施の形態1によるさらに他の携帯電話機の構成を示す概略ブロック図である。

【図9】 図1に示すデータ配信システムにおけるメモリカードの構成を示す概略ブロック図である。

【図10】 図1に示すデータ配信システムにおける配信動作を説明するための第1のフローチャートである。

【図11】 図1に示すデータ配信システムにおける配信動作を説明するための第2のフローチャートである。

【図12】 メモリカードにおける再生リストファイルの構成を示す図である。

【図13】 携帯電話機における暗号化コンテンツデータの再生動作を説明するためのフローチャートである。

【図14】 図13に示す実施の形態1における初期化処理の動作を説明するためのフローチャートである。

【図15】 図13に示す実施の形態1における再生許諾処理の動作を説明するためのフローチャートである。

【図16】 図15に示すフローチャートの一部を差替えるためのフローを示すフローチャートである。

【図17】 実施の形態2による携帯電話機の構成を示す概略ブロック図である。

【図18】 実施の形態2による他の携帯電話機の構成を示す概略ブロック図である。

【図19】 実施の形態2によるメモリカードの構成を示す概略ブロック図である。

【図20】 実施の形態2における再生許諾処理の動作を説明するためのフローチャートである。

【図21】 実施の形態3による携帯電話機の構成を示す概略ブロック図である。

【図22】 実施の形態3による他の携帯電話機の構成を示す概略ブロック図である。

【図23】 実施の形態3によるメモリカードの構成を示す概略ブロック図である。

【図24】 実施の形態3における初期化処理の動作を説明するためのフローチャートである。

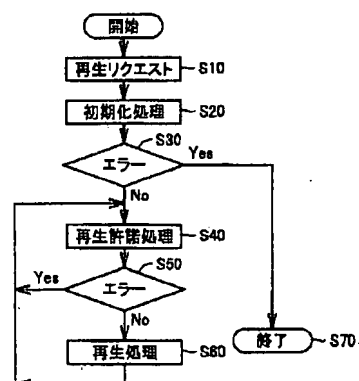
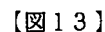
【図25】 実施の形態3における初期化処理の動作を説明するための他のフローチャートである。

【図26】 実施の形態3における再生許諾処理の動作を説明するためのフローチャートである。

【符号の説明】

10 配信サーバ、20 配信キャリア、1, 2, 21 ~ 23 領域、100, 102, 104, 100A, 102A, 100B, 102B 携帯電話機、110, 110A, 110B メモリカード、130 ヘッドホン、160 再生リストファイル、165 エントリ管理情報、302 課金データベース、304 情報データベース、307 メニューデータベース、308 配信記録データベース、310 データ処理部、312, 320, 1404, 1408, 1409, 1412, 1422, 1504, 1510, 1516 復号処理部、313 認証鍵保持部、315 配信制御部、316, 1418, 1508 セッションキー発生部、318, 326, 328, 1406, 1410, 1506 暗号処理部、350 通信装置、1120, 1420 コントローラ、1426, 1530 端子、1100 アンテナ、1102 送受信部、1104 マイク、1106 AD変換部、1108 音声符号化部、1110 音声再生部、1112, 1519 DA変換部、1114 スピーカ、1116 操作パネル、1118 表示パネル、1200 メモリカードインタフェース、1400, 1500 認証データ保持部、1402 Km保持部、1414 KPa保持部、1415 メモリ、1415A ライセンス領域、1415B データ領域、1416 KPmc保持部、1421 Km保持部、1424 インタフェース、1442, 1446 切換スイッチ、1502 Kp保持部、1507, 1507A, 1507B 機能証明書保持部、1512 時計、1514 再生制御部、1518 音楽再生部、1521 ~ 1525, 1621 ~ 162n ライセンス管理ファイル、1531 ~ 1535, 1611 ~ 161n コンテンツファイル、1550 コンテンツ再生デバイ

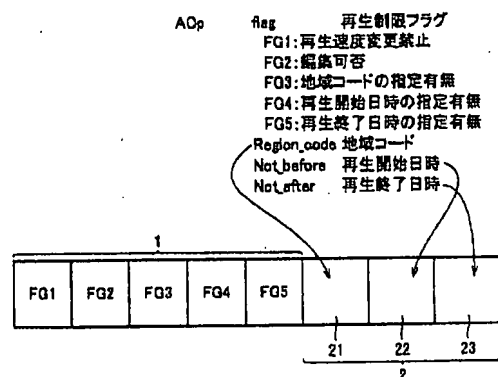
【圖 1】



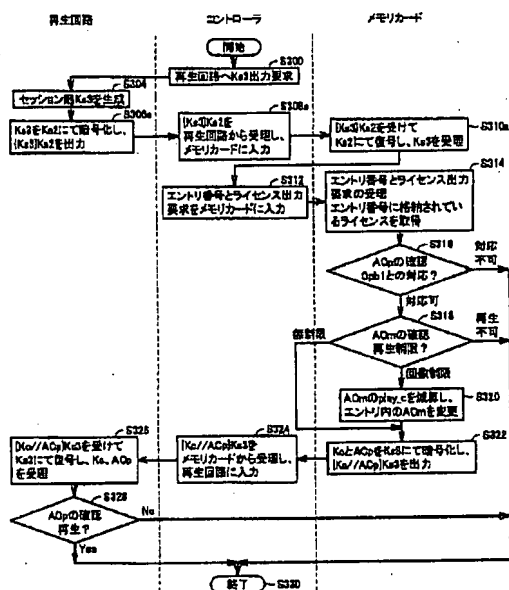
【圖2】

| 記号      | 種類       | 属性      | 特性   |
|---------|----------|---------|--|
| Do      | コンテンツデータ | コンテンツ固有 | 例:音楽データ、朗読データ、教材データ、画像データ<br>Keにて番号可能な暗号化コンテンツデータ<br>ID Keとして配信され、メモリカードに保持される |
| De-Inf  | 付加情報     | コンテンツ固有 | Deに付随する平文データ。  |
| Ke      | ライセンス    | コンテンツ固有 | ライセンス<br>暗号化コンテンツデータを番号する番号鍵   |
| ACm/AOp | ライセンス    | ライセンス固有 | 制限情報<br>再生やライセンスの取り扱いに対する制限事項  |
| コンテンツID | ライセンス    | コンテンツ固有 | コンテンツを特定するための管理コード   |
| ライセンスID | ライセンス    | ライセンス固有 | ライセンスを特定するための管理コード   |
| ライセンス   | ライセンス    | ライセンス固有 | Ke + ACm + AOp + コンテンツID + ライセンスIDの総称  |

【圖3】



【圖26】



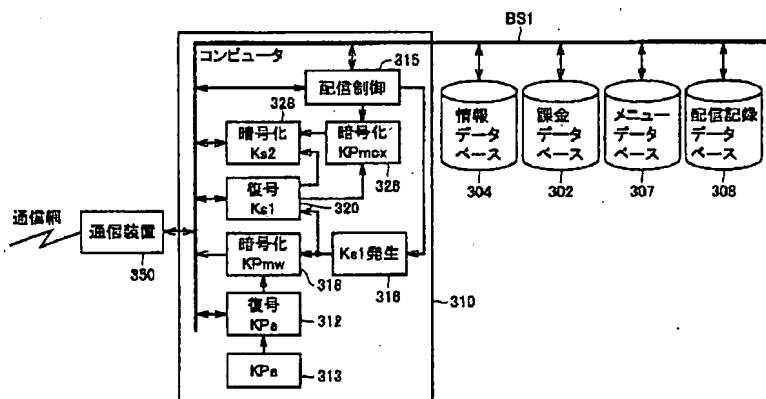


【図4】

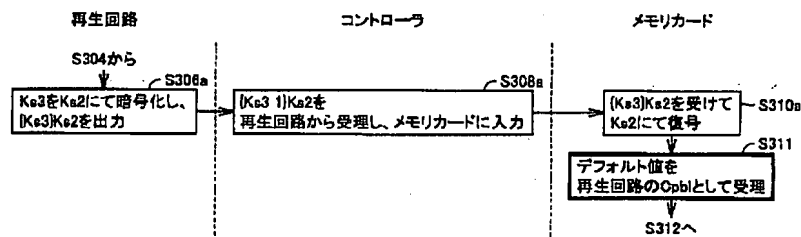
|             | 記号    | 種類    | 属性      | 特性  |
|-------------|-------|-------|---------|---|
| 配信サーバ       | KPa   | 公開証文  | システム共通  | 証証局にて証証データを値とする   |
|             | Ka1   | 共通鍵   | セッション固有 | メモリカードへのライセンス配信ごとに発生  |
| メモリカード      | KPa   | 公開証文  | システム共通  | 証証局にて証証データを値とする<br>※配信サーバのKPaと同一  |
|             | KPmw  | 公開暗号鍵 | クラス固有   | 証明書Cmwとともに証証局にて暗号化された証証データとして保持<br>※kはクラスを識別するための識別子                                  |
|             | Krmw  | 秘密暗号鍵 | クラス固有   | 公開暗号鍵KPmwにて暗号化されたデータを値とする非対称な値暗号  |
|             | KPmcx | 公開暗号鍵 | 値別      | メモリカードごとに異なる。<br>※kはモジュールを識別するための識別子  |
|             | Krmcx | 秘密暗号鍵 | 値別      | 公開暗号鍵KPmcxにて暗号化されたデータを値とする非対称な値暗号   |
|             | Ka2   | 共通鍵   | セッション固有 | 配信サーバまたは音楽再生スケジュール間のライセンスの授受ごとに発生   |
|             | Cmw   | 証明書   | クラス証明書  | メモリカードのクラス証明書。<br>証証機能を有する。<br>①KPmw//Cmw/KPaの形式で出荷時に記録。<br>※メモリカードのクラスごとに異なる。        |
| コンテンツ再生デバイス | KPpy  | 公開暗号鍵 | クラス固有   | 証明書Cmwとともに証証局にて暗号化された証証データとして保持<br>※kはクラスを識別するための識別子                                  |
|             | Kpy   | 秘密暗号鍵 | クラス固有   | 公開暗号鍵KPpyにて暗号化されたデータを値とする非対称な値暗号  |
|             | Ka3   | 共通鍵   | セッション固有 | 配信サーバまたは音楽再生スケジュール間の再生セッションごとに発生  |
|             | Opay  | 証明書   | クラス証明書  | コンテンツ再生デバイスのクラス証明書。証証機能を有する。<br>①KPpy//Opay/KPaの形式で出荷時に記録。<br>※コンテンツ再生デバイスのクラスごとに異なる。 |
|             | Opbi  | 証明書   | 機能証明書   | コンテンツ再生デバイスの機能証明書。<br>OpbiまたはOpbi/KPpyの形式で出荷時に記録。<br>※コンテンツ再生デバイスのクラスごとに異なる。          |

【圖 5】

**10**

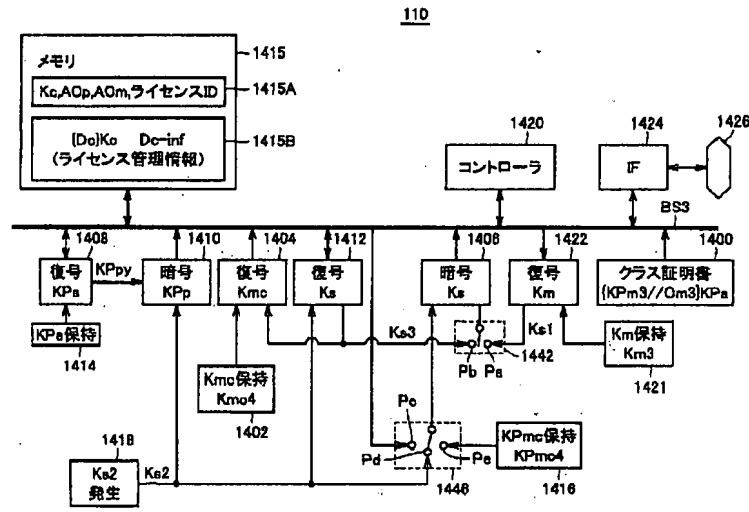


【圖 16】

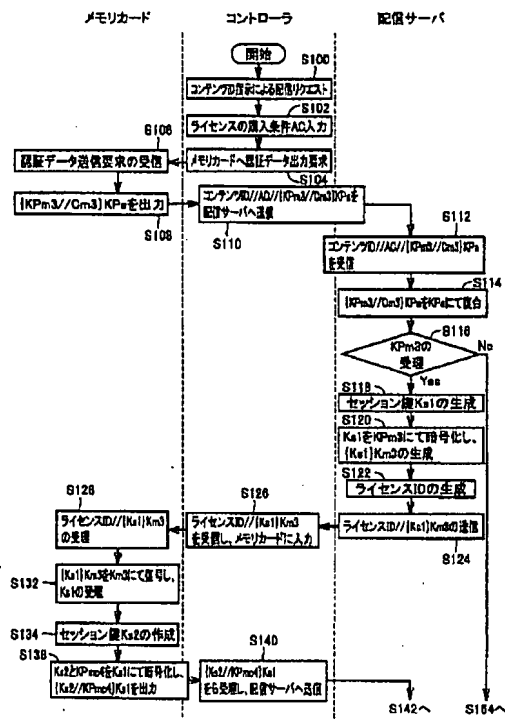


[illegible][illegible]

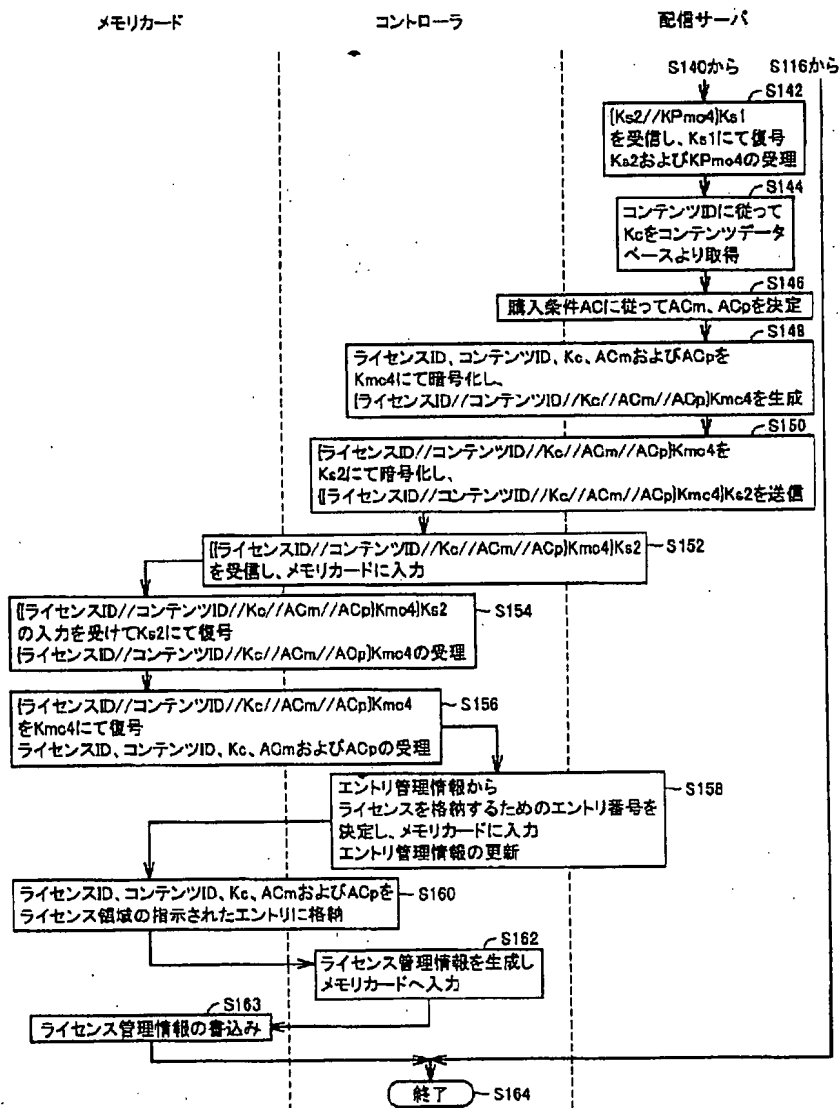
【図9】



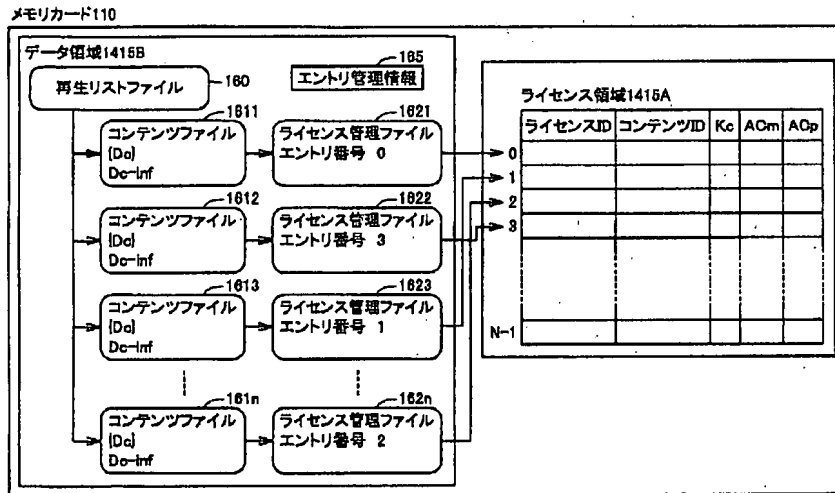
【図10】



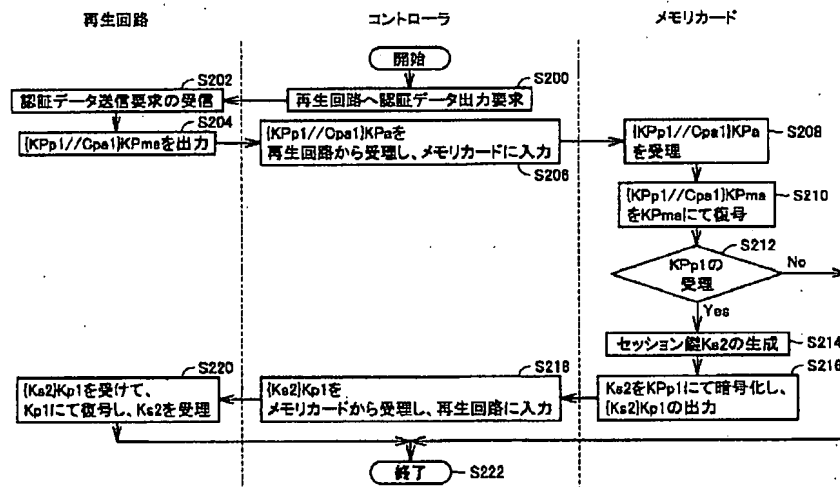
【図11】



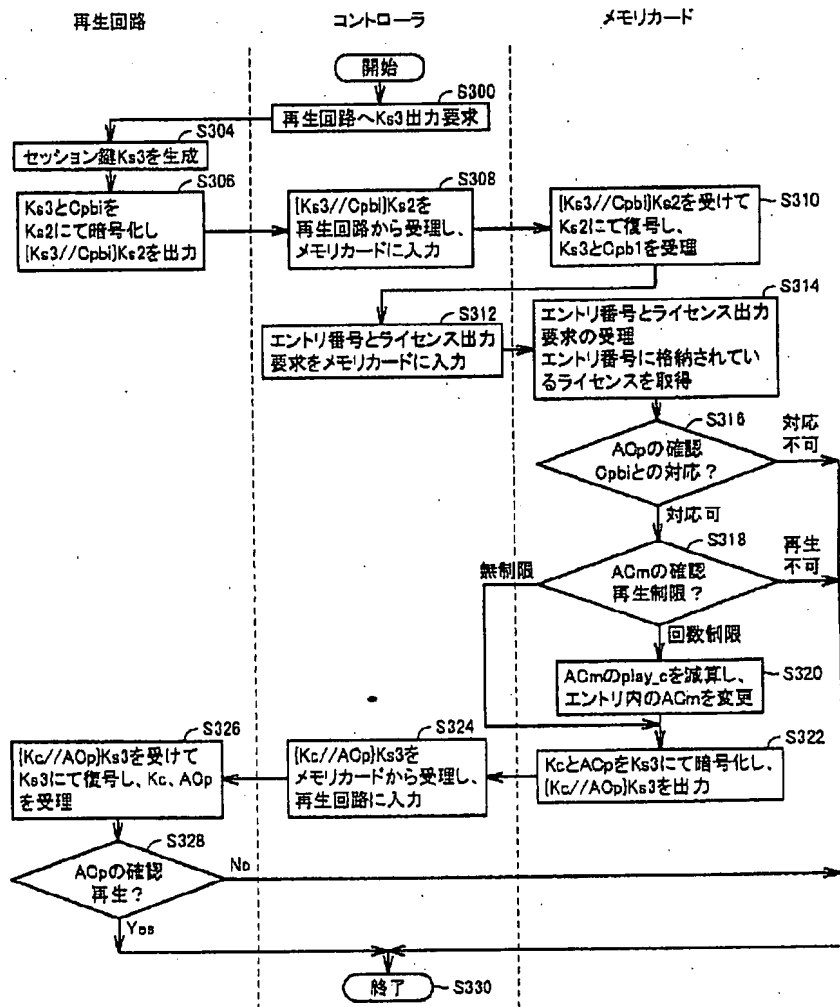
【図12】



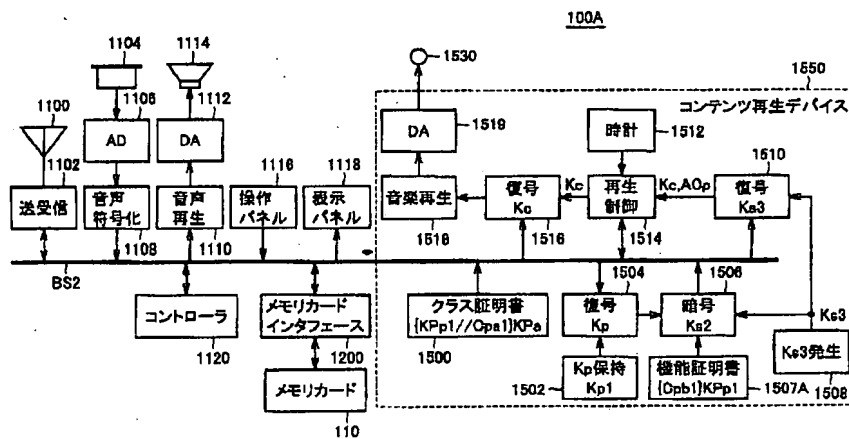
【図14】



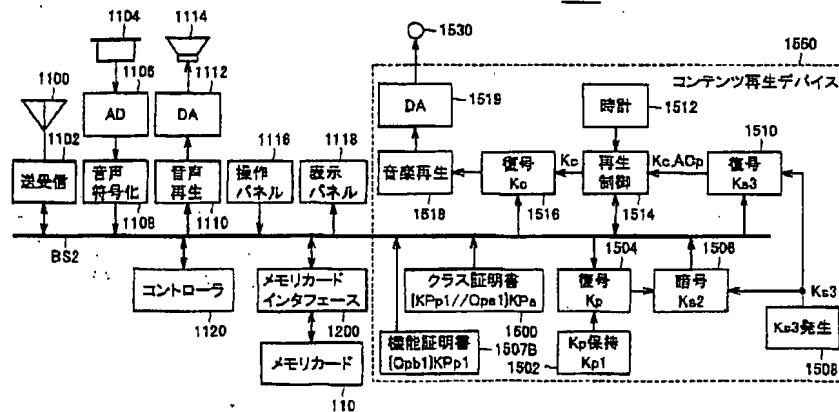
【図15】



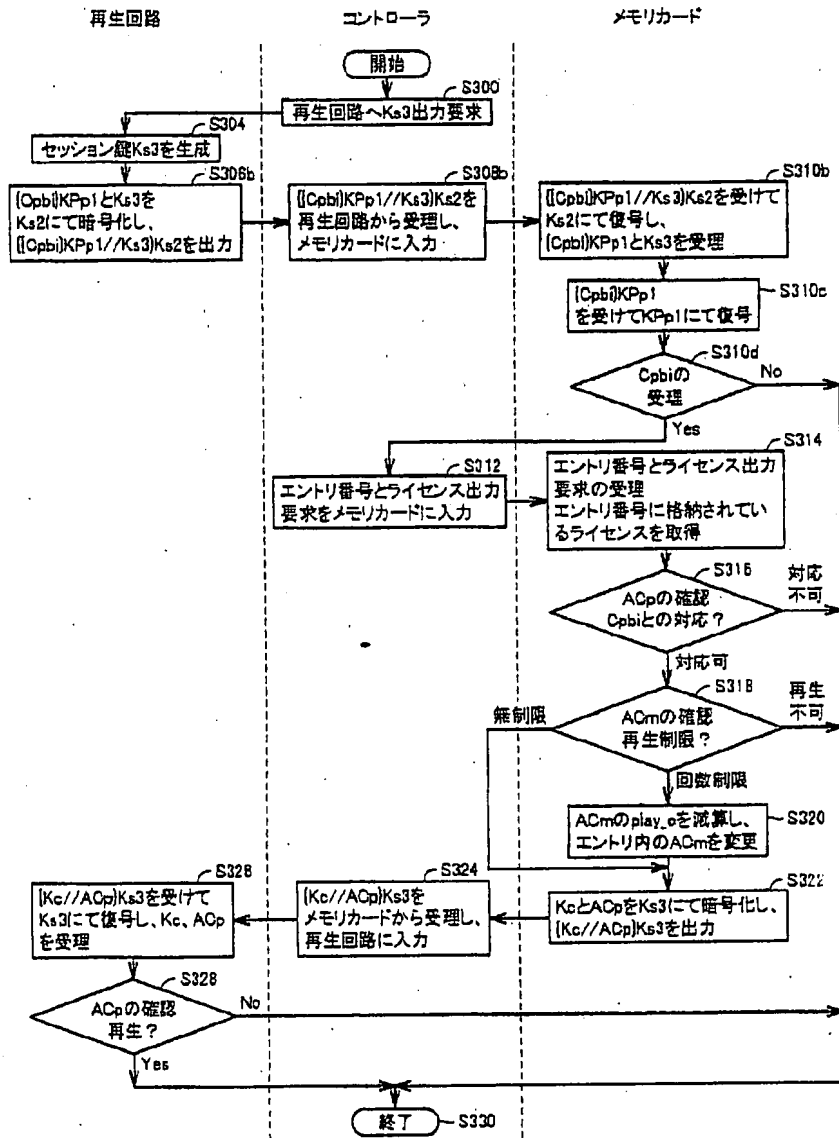
【図17】



**102A**

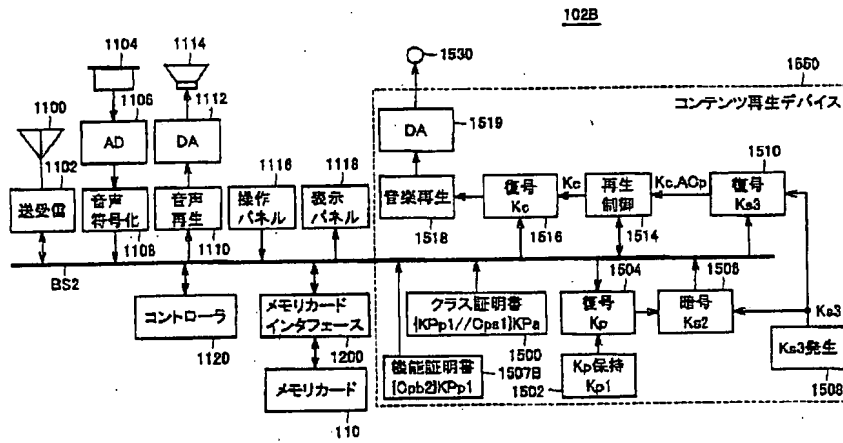


【図20】

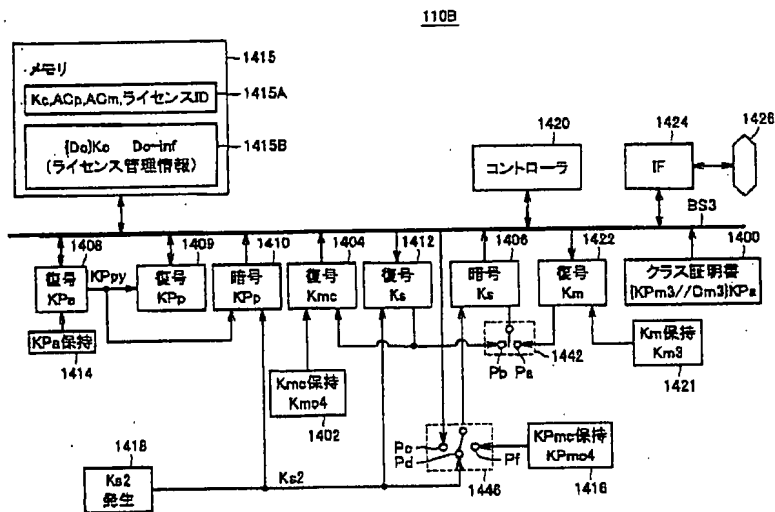




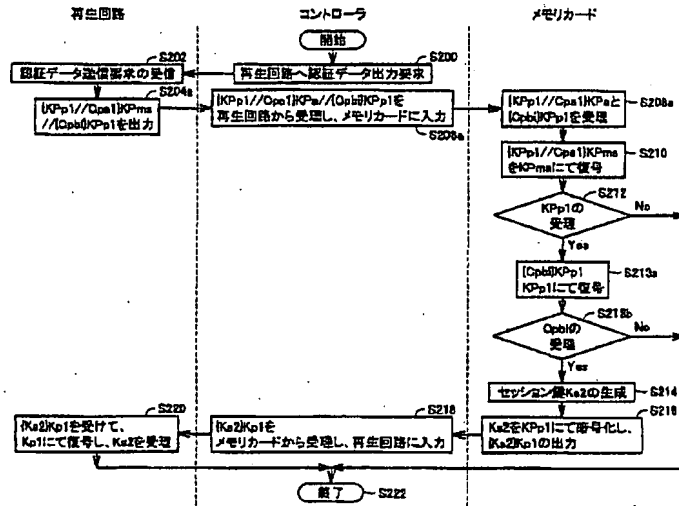
【図22】



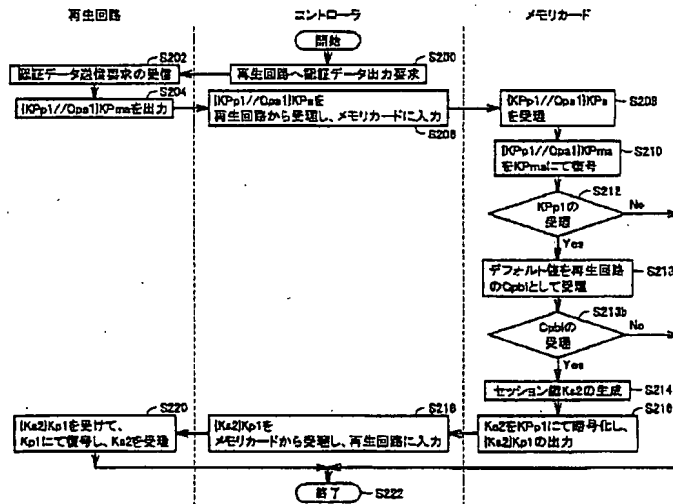
【図23】



【図24】



【図25】



フロントページの続き

(51)Int.Cl.

識別記号

FI

テーマコード(参考)

H04N 7/167

H04N 7/167

Z 5J104

// H04N 5/765

H04L 9/00

601B 5K101

5/907

H04N 5/91

L

5/91

P

Fターム(参考) 5B017 AA07 BA07 BB10 CA16  
5B035 AA13 BB09 BC00 CA11 CA38  
5C052 GA08 GB01 GB07 GC00 GE08  
5C053 FA13 FA27 GB40 LA15  
5C064 BA01 BB01 BC04 BC23 BC25  
BD02 CB01 CC04  
5J104 AA01 AA16 EA01 EA04 EA22  
NA02 PA14  
5K101 KK18 LL01 LL11